

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

USDC SDNY DOCUMENT ELECTRONICALLY FILED DOC #: DATE FILED: <u>5/26/2021</u>
---

UNITED STATES OF AMERICA,

-v-

LAWRENCE RAY,

Defendant.

-----X  
:  
:  
:  
:  
:  
:  
:  
:  
:  
:  
:  
:  
-----X

20-cr-110 (LJL)

OPINION & ORDER

LEWIS J. LIMAN, United States District Judge:

Defendant Lawrence Ray (“Ray”) moves, pursuant to Federal Rule of Criminal Procedure 12, to suppress evidence seized pursuant to a search warrant. The motion is denied.

## BACKGROUND

### A. The Indictment

On February 6, 2020, a Grand Jury sitting in this District returned Indictment 20 Cr. 110 (the “Indictment”). Dkt. No. 2. The Indictment charged Defendant Lawrence Ray with nine counts: Extortion Conspiracy in violation of 18 U.S.C. § 1951 (Count One), Extortion in violation of 18 U.S.C. §§ 1951, 1952 (Count Two), Sex Trafficking in violation of 18 U.S.C. §§ 1591, 1592 (Count Three), Forced Labor in violation of 18 U.S.C. § 1589, 1582 (Count Four), Forced Labor Trafficking in violation of 18 U.S.C. §§ 1590, 1592 (Count Five), Forced Labor Conspiracy in violation of 18 U.S.C. § 1594 (Count Six), Use of Interstate Commerce to Promote Unlawful Activity in violation of 18 U.S.C. § 1952(a)(3) (Counts Seven and Eight), and Money Laundering in violation of 18 U.S.C. §§ 1956(a)(1)(B)(i) and 2 (Count Nine). Dkt. No. 2 at 10-19.

The Indictment alleges that Ray targeted a group of college students and others for indoctrination and criminal exploitation, including extortion, forced labor, and prostitution. *See* Dkt. No. 2 at 1 (“Over the course of nearly a decade, between in or about 2010 through the present, RAY subjected the Victims to sexual and psychological manipulation and physical abuse.”). He is accused of extracting from at least seven victims false confessions that they had caused harm and damage to Ray and to his family members and associates *Id.* He then leveraged the victims’ false confessions to extort money from the victims, to force some of the victims to perform unpaid manual labor, and to cause one of the female victims to engage in commercial sex acts for Ray’s financial benefit. *Id.* at 1-2. The Indictment includes examples of Ray’s alleged physical threats to certain of the victims, his use of the false confessions to force the victims to pay him hundreds of thousands of dollars, his use of verbal and physical threats to force the victims to perform work on a project owned by a Ray family member, and his inducement of one victim to act as a prostitute. *Id.* at 2-9. He is also alleged to have laundered the proceeds of his criminal activity. *Id.* at 9-10.

On January 26, 2021, the Grand Jury returned a superseding Indictment (the “Superseding Indictment”) charging Ray with Racketeering Conspiracy, in violation of 18 U.S.C. § 1962(d) (Count One), Extortion Conspiracy in violation of 18 U.S.C. § 1951 (Count Two), Extortion in violation of 18 U.S.C. §§ 1951 and 2 (Count Three), Sex Trafficking in violation of 18 U.S.C. §§ 1951 and 2 (Count Four), Conspiracy to Commit Sex Trafficking in violation of 18 U.S.C. § 1594 (Count Five), Forced Labor in violation of 18 U.S.C. §§ 1589 and 2 (Count Six), Forced Labor Trafficking in violation of 18 U.S.C. §§ 1590 and 2 (Count Seven), Forced Labor Conspiracy in violation of 18 U.S.C. § 1592 (Count Eight), Use of Interstate Commerce To Promote Unlawful Activity in violation of 18 U.S.C. §§ 1952(a)(3)(B) and 2

(Count Nine), Use of Interstate Commerce to Promote Unlawful Activity in violation of 18 U.S.C. §§ 1952(a)(3)(B) and 2 (Count Ten), Money Laundering in violation of 18 U.S.C. §§ 1956(a)(1)(B)(i), (ii), and 2 (Count Eleven), and Tax Evasion for the years 2015 (Count Twelve), 2016 (Count Thirteen), 2017 (Count Fourteen), 2018 (Count Fifteen), and 2019 (Count Sixteen). Dkt. No. 127. The Superseding Indictment added as Isabella Pollok as a defendant.

## **B. The Search Warrants**

Ray's motion challenges several search warrants obtained during the investigation of his alleged crimes.

### **1. The Cell Site Warrant**

On July 26, 2019, the Government obtained a warrant for historical cell site location information ("CSLI") for three phone numbers, including one ending with the digits 9122. Dkt. No. 112-1 at 18-20. The warrant ordered Ray's telephone service provider to supply "all available historical cell cite location information reflecting the cell towers and sectors thereof utilized in routing any phone, text, or data communication to or from the Target Cellphone, and the approximate range of the target phone from the cell towers during the communication . . . , for the period from June 1, 2013 through the date of th[e] Order, as well as all available toll records (including call detail, SMS detail, or data session detail records) for the communications." Dkt. No. 112-1 at 19. Based on the warrant, the Government received data spanning July 29, 2018 through July 26, 2019 for the 9122 cellphone. It received data dating back to 2013 for the other phones. Dkt. No. 161 at 3.

The CSLII Warrant (the "CSLI Search Warrant") was signed by Magistrate Judge Stewart Aaron on July 26, 2019. Dkt. No. 112-1 at 20. Judge Aaron's order supporting the warrant recited the Court's findings that the cell phone ending in 9122 was "subscribed to in the

name of Lawrence Greco,”—the birth name of Lawrence Ray—that the “Government’s application set[] forth probable cause to believe that the historical location information for the Target Cellphone . . . w[ould] reveal evidence, fruits, or instrumentalities of suspected violations of 18 U.S.C. §§ 1962 (racketeering conspiracy), 1591 (sex trafficking), 1594 (sex trafficking conspiracy), 1589 (forced labor . . .),” and that there were “reasonable grounds to believe that the historical location information and toll records for the Target Cellphone . . . [would be] relevant and material to an ongoing criminal investigation.” *Id.* at 18-19.

The warrant’s probable cause finding was based on facts contained in an affidavit signed by Special Agent Kelly Maguire (“SA Maguire”) of the Federal Bureau of Investigation (“FBI”) (the “CSLI Search Warrant Affidavit”). Dkt. No. 112-1 at 7-17. SA Maguire identified her qualifications and experience. *Id.* at 7-8. She had been an FBI Special Agent assigned to the Child Exploitation and Human Trafficking Task Force for approximately a year and a half, having previously served in Special Operations for the Joint Terrorism Task Force. *Id.* at 7. Prior to joining the FBI, she was a “Detective/Police Officer” in the Charleston Police Department in Charleston, South Carolina for approximately 9 years and had served in its Special Investigations Unit, which encompassed investigations of narcotics, vice, and violent crimes against children. *Id.* Based on her experience, SA Maguire was “familiar with investigative techniques regarding cellphones and other technology to commit federal crimes” and had “experience executing search warrants, including warrants for cellphone location data.” *Id.*

The CSLI Search Warrant Affidavit set forth facts establishing probable cause that the historical location information and toll records for the 9122 cellphone, as well as the two other cellphones, would lead to evidence of violations of 18 U.S.C §§ 1962 (racketeering conspiracy),

1591 (sex trafficking), 1594 (sex trafficking conspiracy), and 1589 (forced labor). *Id.* at 10-16. The facts included information contained in a New York Magazine article entitled “The Stolen Kids of Sarah Lawrence,” published on or about April 28, 2019 (the “Article”). *Id.* at 10-11. Among the facts recited in the Article were: (1) that on or about September 2010, following his release from prison, Ray moved in with his daughter Talia Ray and her roommates at Sarah Lawrence College (the “Roommates”); (2) that “[o]ver time, [he] began to control aspects of the lives of some of the Roommates;” (3) that he gave “counseling sessions” to one of the women, Female Victim-1 (“FV-1”) and “sexual education” to some Roommates; (4) that he brought FV-1 and others to his stepfather’s house in Pinehurst, North Carolina to install a drainage system in the yard; (5) that Ray has created a website that documented purported confessions from FV-1 including that she had tried to poison Ray; (6) that in 2014 FV-1 had begun working as an escort and would give her profits to Ray in order to pay for the damage she had done to Ray’s property; (7) that Ray had admitted to the author of the article that he had taken the money FV-1 had earned from escorting and was pleased with her efforts to pay him back for the damage he says she did; and (8) that FV-1 had told a former-employer that Ray had strapped her to a chair and put a plastic bag over her head. *Id.* at 10-14.

The affidavit also included corroborating information obtained by SA Maguire through interviews she conducted with FV-1 beginning in June 2019. FV-1 did not supply the information in the Article but had fact checked portions of it for the author. *Id.* at 12-14. The corroborating information supplied by FV-1 included: (1) that Ray had moved in with FV-1, Talia Ray, Isabella Pollok, Santos Rosarios and others, while they were students at Sarah Lawrence College; (2) that Ray had provided some of the Roommates with “sex education” and that he had provided FV-1 with “counseling sessions;” (3) that Ray had repeatedly asked FV-1

“why she was poisoning him and others;” (4) that FV-1 had “started to believe that she had in fact poisoned Ray and others and had ‘confessed’ to it at Ray’s urging,” including by recording on Ray’s iPhone a confession which was later posted on YouTube; and (5) that FV-1 “no longer believe[d] she poisoned Ray or anyone else.” *Id.* at 12. The CSLI Search Warrant Affidavit recited further information reported by FV-1, including: (6) that she had travelled to Pinehurst, North Carolina for about six weeks around Father’s Day 2013 to do work in the backyard of Ray’s stepfather’s house; (7) that, while she was doing physical labor in the backyard, Ray controlled her access to food and sleep and on one occasion shoved her down and berated her for intentionally doing bad work in the yard; and (8) that, on another occasion, Ray had left her to sleep outside and denied her food for more than a day. *Id.* at 12-13.

FV-1 also stated in the FBI interviews that Ray had created a website that contained negative information about FV-1 (which he told FV-1 he had created because she had behaved poorly), including the statement that she had poisoned him. *Id.* at 13. FV-1 also stated during the FBI interviews that Ray “routinely threatened” to turn her into the police for poisoning him. *Id.* The CSLI Search Warrant Affidavit further stated that FV-1 told the FBI, consistent with the information in the Article, that Ray had suggested to FV-1 that she work as an escort and that she could repair the damage she had done, including the damage done by poisoning him, by giving him the proceeds from escorting. *Id.* FV-1 told the FBI that Ray had, in fact, picked up escorting proceeds from her and “pressured [FV-1] to see more clients and to charge higher prices in order to make greater repairs to Ray for the damage she had done. *Id.* The CSLI Search Warrant Affidavit recited an occasion during which Ray had threatened to kill FV-1 and told her to “behave and focus on repairs,” which she understood to mean that she should continue working as an escort and providing the proceeds to Ray. *Id.* at 13-14. The affidavit

recited that in or about April 2019, Ray spoke to FV-1 about the impending Article and asked her to meet with him so that they could speak to the author together. *Id.* at 14. Instead, with the aid of a former employer, FV-1 ran away. *Id.*

The affidavit contained facts supplying probable cause that the 9122 cellphone was used by Ray. *Id.* at 14-16. The evidence included that that the cellphone ending with the digits 9122 was subscribed in the name of Lawrence Greco, FV-1's identification of that cell phone number was Ray's, and a GoDaddy account belonging to Ray that lists the cell phone number ending in 9122 as his number. Dkt. No. 112-1 at 14. According to the affidavit, there was probable cause to believe that the two other cellphones, Target Cellphone-2 and Target Cellphone-3, were associated with Pollok and FV-1, respectively. *Id.* at 15.

Based on her review of toll records from all three cell phones, SA Maguire concluded that the three phones communicated, so the three users of the phones knew each other. *Id.* at 15. SA Maguire believed that the cell phone data would corroborate the relationship between Ray, Pollak, and FV-1 by placing them at the same locations at salient times based on the facts alleged in the Article and FV-1's FBI testimony. *Id.* at 15-16.2.

## 2. The Email and iCloud Warrants

In September 2019, the Government obtained warrants for seven email accounts maintained by Google, LLC and Apple, Inc., including accounts with the names larryray5@me.com ("Subject Account-7"), lvr.godaddy@gmail.com ("Subject Account-1"), lvr.21@gmail.com ("Subject Account-2"), and lvr.website@gmail.com ("Subject Account-3"). *Id.* at 72-76, 109-120; as well as two accounts believed to be operated by Isabella Pollok ("Subject Account-4" and "Subject Account-5") and one account believed to be operated by FV-2 ("Subject Account-6").

The application for a search warrant was supported by affidavits from SA Maguire (the “Email Search Warrant Affidavits”). *Id.* at 77-108. The Email Search Warrant Affidavits set forth facts supporting the existence of probable cause to believe that the email accounts would contain evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 1589 (forced labor), 1590 (trafficking with respect to forced labor), 1591 (sex trafficking through force, fraud, or coercion), 1594(b) (conspiracy to commit forced labor or trafficking with respect to forced labor), 1594(c) (conspiracy to commit sex trafficking through force, fraud, or coercion), 1552 (Travel Act), 371 (conspiracy to violate the Travel Act), 1556(a) (money laundering), 1556(h) (conspiracy to commit money laundering), 1551 (extortion), and 1591 *et seq.* (racketeering) (collectively, “Email Subject Offenses”). *Id.* at 78-79.

The facts set forth in the Email Search Warrant Affidavits included information from the Article, the citation and website information for which were included in the Email Search Warrant Affidavits. *Id.* at 84. The information from the Article included the facts that were set forth in the CSLI Search Warrant Affidavit, including (1) that in late September 2010, Ray moved into an on-campus dormitory with Talia Ray and several others, including FV-1; (2) that Ray conducted “counseling” sessions with the Roommates and “coached [certain of the individuals] through sex”; (3) that Ray required the Roommates and others to write and deliver to him handwritten confessions regarding ways in which they had intentionally harmed Ray; (4) that Ray brought FV-1 and some of the other Roommates to Ray’s stepfather’s house in Pinehurst, North Carolina where he put them to work installing a new drainage system in the yard and convinced FV-1 that she had damaged the property during the work and owed him money; (5) that in 2013 FV-1 began working as an escort and giving Ray the profits in order to pay for the damage he had convinced her that she had done to his stepfather’s property in North



Carolina; (6) that Ray had admitted to the author of the article that he had taken money that FV-1 had earned from working as an escort and was pleased with FV-1's efforts to pay him back for his damages; (7) that Ray had convinced FV-1 (and one other person) that they had poisoned him and created a website documenting FV-1's confession to poisoning Ray and Ray's daughter; and (8) that Ray had physically threatened FV-1. *Id.* at 84-88.

The Email Search Warrant Affidavits also contained information from the FBI's interview of FV-1, whose information SA Maguire stated "has been credible and corroborated in part by independent evidence." *Id.* at 88 n.2. The information from FV-1's FBI interviews cited in the Email Search Warrant Affidavits was consistent with (but more extensive than) the information from FV-1 reported in the CSLI Search Warrant Affidavit. It included that Ray had shown FV-1 documents that looked like medical records pertaining to his mercury levels during the time he was alleging that FV-1 was poisoning him, and that FV-1 wrote multiple draft confessions which she emailed to Ray. *Id.* at 92. FV-1 had also seen similar written confessions from others among Ray's victims. *Id.* According to the Email Search Warrant Affidavits, Ray threatened to bring FV-1's poisoning confessions to law enforcement if she did not provide him with more money. *Id.* at 93. FV-1 additionally stated that, while she was in Pinehurst, Ray made her work approximately 18 hours per day and allowed her to eat only two meals per day, causing her to lose approximately 30 to 40 pounds during the six weeks they were there. *Id.* at 91. The Email Search Warrant Affidavits included that FV-1 was "using illegal drugs, suffered from insomnia, and was struggling with other personal issues, including interpersonal problems with her parents" at the time she began living with Talia Ray. *Id.* at 89.

As detailed in the Email Search Warrant Affidavits, the information provided by FV-1 and the Article about FV-1's commercial sex acts was corroborated by text messages between

FV-1 and another Roommate related to the commercial sex acts and by advertisements for FV-1 which were posted on numerous websites which host advertisements for commercial sex *Id.* at 95. The Email Search Warrants also discussed records obtained from GoDaddy and certain financial institutions showing payments from FV-1 and another Roommate to Ray, as well as records obtained from PayPal showing the receipt of what appear to be prostitution proceeds by FV-1 and large cash withdrawals which corresponded to transfers of those proceeds to other individuals. *Id.* at 95-98.

The Email Search Warrant Affidavits also included extensive evidence of crimes involving the other alleged victims. These included allegations of physical and sexual abuse of other victims. *Id.* at 86-87. The Email Search Warrant Affidavit included reporting from the Article that Ray had threatened to dismember Male Victim-1 while brandishing a knife at him, and that he, on one occasion, put Male Victim-2 in a “sleeper” hold until he passed out. *Id.* at 87. It also included the testimony of FV-1 that Pollok worked as an escort and prostitute on behalf of Ray. *Id.* at 94.

The Email Search Warrant Affidavits contained specific facts showing that Subject Accounts-1, -2, -3 and -7 were used by Ray. Subject Account-1 was registered to Lawrence Ray and was used to register GoDaddy domains for an account in the name of Lawrence Ray, created in March 2011. *Id.* at 98. This account was associated with the phone number FV-1 identified as Ray’s phone number. *Id.* at 99. Subject Account-2 was used in updated billing information for the same GoDaddy account, along with the phone number. Subject Account-3 was used in updated billing information provided to GoDaddy for a domain registered to Ray’s GoDaddy Account. *Id.* It was also associated with a PayPal account in Ray’s name, that was also

registered to Ray's phone number. *Id.* Subject Account-7 was registered to the name Larry Ray. FV-1 identified Subject Account-7 as an account Ray had used to contact her. *Id.* at 100.

The Email Search Warrant Affidavit also included facts showing that Subject Accounts-4 and -5 were used by Isabella Pollok. Subject Account-4 was subscribed in the name "Isabella Pollok" and to a phone number subscribed in the name "Isabella Pollok" and to Ray's mailing address. *Id.* at 100. Subject Account-4 was provided as part of the billing information for Ray's GoDaddy Account. *Id.* Subject Account-5 was associated with a PayPal account in the name Isabella Pollok, which was also associated with Ray's mailing address. *Id.* This PayPal account received nearly \$8,000 in payments from Ray's PayPal account in July 2019. *Id.*

The Email Search Warrant Affidavit included facts showing that Female Victim-2 ("FV-2") was the user of Subject Account-6. *Id.* Subject Account-6 was associated with a GoDaddy account in the name of FV-2 and with a phone number subscribed in FV-2's name and Ray's mailing address. Among the domain names associated with the GoDaddy account was one that combined FV-2 and Ray's names.

The Email Search Warrant Affidavits described email header information for some of the accounts that the Government obtained pursuant to an application under the Stored Communications Act, 18 U.S.C. § 2703(d), and which showed extensive communication with victims and co-conspirators and communications in furtherance of the subject offenses, including communications with FV-1. *Id.*

Magistrate Judge Robert H. Lehrburger authorized the Email Search Warrants (the "Email Search Warrants") on September 23, 2019. *Id.* at 72-73, 109-110. Judge Lehrburger's order recited his finding of probable cause to believe that the email accounts "contain[ed] evidence, fruits, and instrumentalities of crime," that the providers were directed to provide

certain information specified in the warrant to law enforcement “for subsequent review by law enforcement personnel as authorized [in the warrant].” *Id.* at 72, 109. The warrants limited the search of the email accounts to the period from January 1, 2011 through the date of the warrant for four of the accounts, to the period from July 1, 2012 through the date of the warrant for one of the accounts, and to the period from January 1, 2015 through the date of the warrant for two of the accounts. *Id.* at 75, 114. Law enforcement were “authorized to review the records to locate any evidence, fruits, and instrumentalities [of the Email Subject Offenses],” including 12 different categories of evidence. *Id.* at 75.

In the Email Search Warrant Affidavits, SA Maguire had represented:

In conducting this review, law enforcement personnel may use various methods to locate evidence, fruits, and instrumentalities of the Subject Offenses, including but not limited to undertaking a cursory inspection of all emails within the Subject Accounts. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with emails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account, as it is impossible to know in advance all of the unique words or phrases that investigative subjects will use in their communications, and consequently there are often many communications in an account that are relevant to an investigation but that do not contain any keywords that an agent is likely to search for.

*Id.* at 106-07. Accordingly, the Email Search Warrant did not require law enforcement to use keyword searching to limit the scope of the search. Instead, the Warrant stated that “law enforcement may use various techniques to determine which files or other ESI contain evidence or fruits of the Subject Offenses.” Dkt. No. 110-1 at 248. Such techniques could include:

- Surveying various file ‘directories’ and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it

- contains and opening a drawer believed to contain pertinent files);
- Opening or cursorily reading the first few ‘pages’ of such files in order to determine their precise contents;
- Scanning storage areas to discovery and possibly recover recently deleted files or deliberately hidden files;
- Performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and
- Reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

*Id.* at 248-49.

On October 7, 2019, SA Maguire filed an affidavit in support of a search warrant for various iCloud accounts (“iCloud Search Warrant Affidavit”). *Id.* at 128-156. The iCloud Search Warrant Affidavit was substantially identical to the Email Search Warrant Affidavits. *Id.* On October 7, 2019, Magistrate Judge Ona Wang signed the iCloud Search Warrant. *Id.* at 157-65. The iCloud Search Warrant authorized the Government to seize evidence, fruits and instrumentalities of the Email Subject Offenses “involving Lawrence Ray since in or about 2010,” including 11 categories of information. *Id.* at 163. The warrant recited:

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

*Id.* at 165.

### 3. The Premises Warrants

On February 7, 2020, the Hon. Cathy L. Waldor of the District of New Jersey authorized a search warrant for Ray’s residence at 40 Holly Lane, Piscataway, New Jersey (the “40 Holly

Lane Premises”), *id.* at 243-49, “includ[ing] all locked and closed containers found therein, as well as any computers, mobile devices, electronic devices, or electronic storage media found therein.” *Id.* at 245 (the “Premises Search Warrant”). The Premises Search Warrant authorized a search for evidence of the following Subject Offenses (the “Premises Subject Offenses”): 18 U.S.C. §§ 1589 (forced labor), 1590 (trafficking with respect to forced labor), 1591 (sex trafficking through force, fraud, or coercion), 1594(b) (conspiracy to commit forced labor or trafficking with respect to forced labor), 1952 (Travel Act), 1956(a) (money laundering), 1951 (extortion), and 26 U.S.C. § 7201 (tax evasion). *Id.* at 246. The warrant listed 12 categories of tangible items that could be seized and searched. *Id.* at 246-249. Those items included electronic devices, all records that referred or related to the receipt, origin, disbursement, or concealment of money and property, and backpacks and their contents. *Id.*

SA Maguire signed the application and affidavit in support of the Premises Search Warrant (“Premises Search Warrant Affidavit”). *Id.* at 250. The affidavit reported that Ray had been indicted by a grand jury and attached a copy of the Indictment, *id.* at 257, which reflected that Ray was charged with committing the Premises Subject Offenses in the time period beginning in or about 2011 and continuing up to the present. The Premises Search Warrant Affidavit summarized that Ray engaged in various forms of criminal conduct, including extracting false confessions from at least seven victims. *Id.* at 260. The Premises Search Warrant Affidavit further alleged that Ray used the false confessions to threaten the victims, in order to obtain purported damages from them, including by telling FV-1 that she could repay the supposed damages she owed to Ray by working as a prostitute. *Id.* at 260-261.

The Premises Search Warrant Affidavit provided the following facts to support probable cause that Ray resided at the 40 Holly Lane address: (1) records from a welfare check conducted

by the Piscataway Police Department (“PPD”) in May 2019 which reported that Ray resided at the 40 Holly Lane Address with one of the victims (FV-2) and an associate (Associate-1); (2) a comparison of videos, some from an iCloud account held by FV-2 and shared by Apple, Inc. in response to the iCloud Search Warrant and others from iCloud accounts of other victims, which show Mr. Ray inside 40 Holly Lane engaged in behavior consistent with residence therein, including preparing food and working on computers; (3) FV-1 informing SA Maguire that Ray was residing in Piscataway, New Jersey with FV-2 when she last contacted him in late 2018; (4) iCloud account information for Associate-1, including text messages to other individuals on May 4, 2019 and August 8, 2019, in which Associate-1 provided 40 Holly Lane as Associate-1’s address; (5) Ray’s iCloud account information including an email from October 2018 in which he asked for his shipping address to be changed to 40 Holly Lane, in the name of Associate-1; (6) records from Uber Technologies, Inc. reflecting that on multiple dates between May 2017 and June 2019, FV-1 and Associate-1 requested rides to and from 40 Holly Lane; (7) reports from law enforcement who observed a vehicle in the driveway of 40 Holly Lane on or about January 31, 2020 which was registered to one of Ray’s relatives; and (8) cellphone location information obtained pursuant to the CSLI Search Warrant reflecting that the cell phone ending in 9122, registered to Ray’s birth name, was within 660 meters of 40 Holly Lane on two dates in February 2020. *Id.* at 262-265.

The Premises Search Warrant Affidavit also contained facts providing probable cause that evidence, fruits and instrumentalities of Ray’s crimes would be found at 40 Holly Lane, including: (1) that Ray maintained handwritten ledgers that would document pick-ups of cash from FV-1; (2) that Ray kept the physical journals in which FV-1 recorded her false confessions; (3) that Ray kept documents which he represented as medical records demonstrating that he had

been poisoned; and (4) that Ray kept large sums of cash in a backpack that he carried with him at all times. Dkt. No. 112-1 at 265-267. SA Maguire also swore that individuals like Ray who use internet-based businesses, such as a domain name business, to facilitate money laundering maintain physical records of their internet businesses and web transactions in and on electronic storage devices or written or printed documents located within their residences. *Id.* at 267-268.

Finally, the Premises Search Warrant Affidavit contained facts supporting probable cause to search electronic devices found at 40 Holly Lane, including evidence that Ray used electronic devices to commit the Subject Offenses by taking and maintaining explicit photographs and “confession videos,” among other things. Dkt. No. 112-1 at 268-274. The evidence to support probable cause was based on SA Maguire’s review of email and iCloud accounts retrieved pursuant to the Email Search Warrant and iCloud Search Warrant from as early as November 2014 and information from FV-1’s cellphones. *Id.* at 269. SA Maguire swore that, based on her experience, individuals who engage in extortion maintain leverage material for years exert control, frighten, and intimidate victims. *Id.* at 271. SA Maguire further asserts that where computers and electronic devices are used in furtherance of criminal activity, evidence of the criminal activity can often be found months or even years after it occurred. *Id.*

With respect to the review of Electronically Stored Information (“ESI”), the Premises Search Warrant recited that law enforcement may use a variety of techniques to determine which files or other ESI contain “evidence or fruits of the Subject Offenses.” *Id.* at 248. Those techniques may include: “surveying various file ‘directories’ and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files)”; “opening or cursorily reading the first few ‘pages’ of such files in order to determine their precise contents”; “scanning storage areas to discover and



possibly recover recently deleted files or deliberately hidden files”; “performing keyword searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation”; and “reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.” *Id.* at 248-49. The Premises Search Warrant further instructed law enforcement personnel make “reasonable efforts” to restrict their search to the specified categories of evidence from the specified time frame, but noted that circumstances may necessitate that law enforcement conduct “a complete review of all the ESI from seized devices or storage media to evaluate its contents and to locate all data responsive to the warrant.” *Id.* at 249.

On the date of Ray’s arrest, law enforcement officials received and executed a search warrant for a separate storage unit (the “Storage Unit”) used by Ray in Piscataway, New Jersey (the “Storage Unit Search Warrant”). The Storage Unit Search Warrant was signed by Magistrate Judge Michael A. Hammer of the United States District Court for the District of New Jersey. *Id.* at 305-312. The Storage Unit Search Warrant authorized law enforcement to search and seize evidence, fruits and instrumentalities of the Title 18 offenses enumerated in the Indictment. *Id.* at 309. Items to be seized included tangible items, “all locked and closed containers” in the unit, as well as “any computers, mobile devices, electronic devices, or electronic storage media found therein.” *Id.* at 308. Law enforcement was permitted to use a variety of techniques to determine which of the electronic files or devices contained evidence or fruits of the offenses, but were required to “make reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant for the time period 2010 to Present.” *Id.* at 311-312.

The Storage Unit Search Warrant was supported by an affidavit signed by Special Agent Kristopher Serra (“SA Serra”) of the FBI (the “Storage Unit Search Warrant Affidavit”). *Id.* at 313-336. The Storage Unit Search Warrant Affidavit attached and described the Indictment. *Id.* at 315-318. The Storage Unit Search Warrant Affidavit recited that Ray was arrested at the 40 Holly Lane address on February 11, 2020; that FV-2 and Associate-1 were with him when he was arrested; and that FV-2 told law enforcement that Ray kept the Victims’ journals (which included their “confessions”) in storage bins in the Storage Unit. *Id.* at 320. It also recited, among other things, that SA Serra had obtained consent of the owner, entered the premises where the Storage Unit was located, and viewed “many locked and closed containers, and a laptop computer that appeared to be an early model Apple laptop” within the Storage Unit. *Id.* at 320-321. The Storage Unit Search Warrant Affidavit contained the same facts supporting probable cause to search electronic devices found in the Storage Unit as were contained in the Premises Search Warrant Affidavit. *Id.* at 324-329.

### **APPLICABLE LEGAL PRINCIPLES**

Ray moves to suppress information seized pursuant to the CSLI Search Warrant, the Email Search Warrants, the iCloud Search Warrant, the Premises Search Warrant, and the Storage Unit Search Warrant. He argues that (1) the affidavit supporting the first three sets of warrants, the CSLI Search Warrant, the Email Search Warrants, and the iCloud Search Warrant, contained materially false and misleading misstatements and omissions and obscured the reliability of their only named source; (2) all five sets of warrants were overbroad and not particularized; and (3) the Premises Search Warrant and the Storage Unit Search Warrant lacked a sufficient nexus between the area to be searched and the asserted probable cause. The Court

first discusses the applicable legal principles. It then applies them to each of the warrants and searches at issue.

#### **A. The Probable Cause Requirement**

The Fourth Amendment provides: “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV. “[P]robable cause is a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules.” *United States v. Falso*, 544 F.3d 110, 117 (2d Cir. 2008) (quoting *Illinois v. Gates*, 462 U.S. 213, 232 (1983)). “The task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place.” *Gates*, 462 U.S. at 238. Moreover, “[a] magistrate’s ‘determination of probable cause should be paid great deference by reviewing courts.’” *Id.* at 236 (quoting *Spinelli v. United States*, 393 U.S. 410, 419 (1969)). “[S]o long as the magistrate had a ‘substantial basis for . . . conclud[ing]’ that a search would uncover evidence of wrongdoing, the Fourth Amendment requires no more.” *Id.* at 236 (quoting *Jones v. United States*, 362 U.S. 257, 271 (1960)).

#### **B. The Particularity Requirement**

The particularity requirement of the Fourth Amendment is addressed to the “specific evil [of] the ‘general warrant’ abhorred by the colonists,” and is meant to prevent the “general, exploratory rummaging in a person’s belongings” that such a warrant permitted. *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971). To satisfy the particularity requirement, a warrant

must (1) “identify the specific offense for which the police have established probable cause”; (2) “describe the places to be searched”; and (3) “specify the items to be seized by their relation to the designated crimes.” *United States v. Ulbricht*, 858 F.3d 71, 99 (2d Cir. 2017) (quoting *United States v. Galpin*, 720 F.3d 436, 445 (2d Cir. 2013)). The key is that the search warrant must enable the executing officer to ascertain and identify with reasonable certainty those items authorized to be searched and seized. *See Groh v. Ramirez*, 540 U.S. 551, 557-59 (2004). In other words, the warrant must be “sufficiently specific to permit the rational exercise of judgment [by the executing officers] in selecting what items to seize.” *United States v. Shi Yan Liu*, 239 F.3d 138, 140 (2d Cir. 2000) (quoting *United States v. LaChance*, 788 F.2d 856, 874 (2d Cir. 1986)). Moreover, the description of the objects to be seized may not be “broader than can be justified by the probable cause upon which the warrant is based.” *Galpin*, 720 F.3d at 446.

### **C. The “good faith” exception**

Under the “good faith exception, the exclusionary rule and its remedy of suppression does not apply where evidence is “obtained in objectively reasonable reliance on a subsequently invalidated search warrant.” *United States v. Leon*, 468 U.S. 897, 922 (1984). The law encourages law enforcement to obtain warrants and to rely upon them. Suppression of evidence obtained in reliance upon a facially valid warrant would “[p]enaliz[e] the officer for the magistrate’s error,” and thus not “logically contribute to the deterrence of Fourth Amendment violations.” *Id.* at 921. “[S]earches pursuant to a warrant will rarely require any deep inquiry into reasonableness,” *Gates*, 462 U.S. at 267 (White, J., concurring in judgment), for “a warrant issued by a magistrate normally suffices to establish” that a law enforcement

officer has “acted in good faith in conducting the search.” *United States v. Ross*, 456 U.S. 798, 823 n.32 (1982).

“‘The burden is on the government to demonstrate the objective reasonableness of the officers’ good faith reliance’ on an invalidated warrant.” *United States v. Clark*, 638 F.3d 89, 100 (2d Cir. 2011) (quoting *United States v. George*, 975 F.2d 72, 77 (2d Cir. 1992)). Against the “presumption of reasonableness” that attaches to a search pursuant to warrant, *see Clark*, 638 F.3d at 99, in *Leon*, the Supreme Court identified four circumstances where the exception to the exclusionary rule does not apply: (1) where the issuing magistrate has been knowingly misled; (2) where the issuing magistrate wholly abandoned his or her judicial role; (3) where the application is so lacking in indicia of probable cause as to render reliance upon it unreasonable; and (4) where the warrant is so facially deficient that reliance upon it is unreasonable. *Id.* at 100 (quoting *United States v. Moore*, 968 F.2d 216, 222 (2d Cir. 1992)).

#### **D. *Franks* hearings**

Although “a search or seizure pursuant to a warrant is presumed valid,” a defendant may “[i]n certain circumstances,” request an evidentiary hearing to “challenge the truthfulness of factual statements made in the affidavit, and thereby undermine the validity of the warrant and the resulting search or seizure.” *United States v. Awadallah*, 349 F.3d 42, 64 (2d Cir. 2003); *see Franks v. Delaware*, 438 U.S. 154 (1978). “To obtain a *Franks* hearing on a motion to suppress on the basis of alleged misstatements or omissions in a warrant affidavit, a defendant must make a *substantial* preliminary showing that (1) there were intentional misrepresentations or omissions in the warrant affidavit, or, in other words ‘the claimed inaccuracies or omissions are the result of the affiant’s deliberate falsehood or reckless disregard for the truth’; and (2) those misrepresentations or omissions were material, or ‘necessary to the issuing judge’s probable

cause finding.” *United States v. Nejad*, 436 F. Supp. 3d 707, 718-719 (S.D.N.Y. 2020) (quoting *United States v. Rajaratnam*, 719 F.3d 139, 146 (2d Cir. 2013)). “[T]he reviewing court must be presented with credible and probative evidence” that a misstatement or omission “in a [warrant] application was ‘designed to mislead’ or was ‘made in reckless disregard of whether [it] would mislead.’” *Rajaratnam*, 719 F.3d at 154 (quoting *Awadallah*, 349 F.3d at 68). In the case of an omission, recklessness may be inferred “where the omitted information was ‘clearly critical’ to the probable cause determination.” *Rivera v. United States*, 928 F.2d 592, 604 (2d Cir. 1991). It is not sufficient, however, for the movant to show that “a reasonable person would have included the omitted information.” *Rajaratnam*, 719 F.3d at 154. “[T]he inference is particularly inappropriate where the government comes forward with evidence indicating that the omission resulted from nothing more than negligence, or that the omission was the result of a considered and reasonable judgment that the information was not necessary to the [warrant] application.” *Id.* at 155. “[T]o determine materiality, courts should disregard the allegedly false statements, insert the omitted truths, and determine whether there remains a residue of independent and lawful information sufficient to support probable cause.” *Nejad*, 436 F. Supp. 3d at 719 (internal citations and quotation marks omitted). “If, after setting aside the allegedly misleading statements or omissions, the affidavit, nonetheless, presents sufficient information to support a finding of probable cause, the district court need not conduct a Franks hearing.” *United States v. Salameh*, 152 F.3d 88, 113 (2d Cir. 1998). “To determine whether a false statement was necessary to a finding of probable cause, [the court] consider[s] a hypothetical corrected affidavit, produced by deleting any alleged misstatements from the original warrant affidavit and adding to it any relevant omitted information.” *Ganek v. Leibowitz*, 874 F.3d 73, 82 (2d Cir. 2017).

### **E. “Standing” or Fourth Amendment rights**

“Fourth Amendment rights are personal rights [that] may not be vicariously asserted.” *United States v. Haqq*, 278 F.3d 44, 47 (2d Cir. 2002) (quoting *Rakas v. Illinois*, 439 U.S. 128, 133-34 (1978)). A defendant’s Fourth Amendment rights are violated “only when the challenged conduct invaded *his* legitimate expectation of privacy rather than that of a third party.” *United States v. Payner*, 447 U.S. 727, 731 (1980); *see also United States v. Villegas*, 899 F.2d 1324, 1333 (2d Cir. 1990). “[T]he proponent of a motion to suppress has the burden of establishing that his own Fourth Amendment rights were violated by the challenged search or seizure.” *Rakas*, 439 U.S. at 130 n.1.

## **DISCUSSION**

### **A. Ray has Fourth Amendment rights with respect to some but not all of the premises searched**

As an initial matter, the Government argues that Ray lacks standing to object to any of the search warrants at issue. It argued initially that Ray failed to submit any sworn declaration that he had a possessory interest or any Fourth Amendment right in the cellphone assigned the call number ending in 9122 or either of the other two numbers, the seven email accounts, the seven iCloud accounts, the 40 Holly Lane Premises, or the Storage Unit. Dkt. No. 118 at 16. In response, Ray has submitted a sworn declaration. The declaration states that “before [he] was arrested and incarcerated, [he] lived at [the 40 Holly Lane Premises].” Dkt. No. 160 at 6. It also states that he “kept a storage area in a locked facility at 140 West Ethel Road in Piscataway, New Jersey, which [he] expected to remain private,” and that his “phone number was [the cellphone number ending with 9122].” *Id.* He also identifies seven email and iCloud accounts as his. *Id.* The Government responds that the declaration is too vague and conclusory to establish standing.

On a motion to suppress evidence for failure to satisfy the Fourth Amendment, “[t]he defendant ‘bears the burden of proving . . . that he had a legitimate expectation of privacy.’” *United States v. Watson*, 404 F.3d 163, 166 (2d Cir. 2005) (quoting *Rawlings v. Kentucky*, 448 U.S. 98, 104 (1980)). That burden ordinarily is carried by the submission of sworn declarations. *See, e.g., United States v. White*, 2018 WL 4103490, at \*8 (S.D.N.Y. 2018) (“That burden ‘is met only by sworn evidence, in the form of an affidavit or testimony, from the defendant or someone with personal knowledge.’”) (quoting *United States v. Montoya-Eschevarria*, 892 F. Supp. 104, 106 (S.D.N.Y. 1995)).

Ray has satisfied his burden in part. His declaration is sufficient to satisfy his burden with respect to the 9122 telephone number, which was also registered to him, and with respect to the seven email and iCloud accounts. *See United States v. Lauria*, 2020 WL 5743523, at \*5-6 (S.D.N.Y. Sept. 25, 2020) (holding that defendants’ affirmations that certain cell phone and iCloud accounts belonged to them was sufficient to establish standing for a Fourth Amendment challenge); *United States v. Herron*, 2 F. Supp. 3d 391, 400-01 (E.D.N.Y. 2014) (holding that defendant had a legitimate expectation of privacy in a cellphone registered to another individual, where he provided an affidavit stating that he was the sole and exclusive user of that cellphone). Because he has averred that he owns them, he has established a legitimate expectation of privacy with respect to those accounts sufficient to assert his Fourth Amendment rights.

By contrast, Ray has not established that he had a legitimate expectation of privacy with respect to the other two cellphones and with respect to any of the iCloud or email accounts other than those identified in his sworn declaration. *See United States v. Dore*, 586 F. App’x. 42, 46 (2d Cir. 2014) (holding that defendant lacked standing to challenge a search of cellphone information where “he did not submit an affidavit establishing that the cell phones in question



belonged to him or that he had a subjective expectation of privacy in them” or that he had “a privacy interest in the cell phones in some other manner”); *United States v. White*, 2018 WL 4103490, at \*8 (S.D.N.Y. Aug. 28, 2018) (holding that defendant did not have standing to challenge search of Facebook account where defendant failed to show a property or possessory interest); *United States v. Hamlett*, 2018 WL 4656241, at \*5 (D. Conn. Sept. 27, 2018) (finding no standing where defendant did not “offer any testimony to establish that he had an ownership or cognizable property interest in the cellphone at issue.”); *United States v. Mathieu*, 2018 WL 5869642, at \*2 (S.D.N.Y. Nov. 9, 2018) (“Absent any showing that the email accounts belong to [defendant], Defendant has no basis for challenging the warrant on Fourth Amendment grounds.”).

The Court concludes that Ray has submitted sufficient evidence to show that he had a legitimate expectation of privacy with respect to the 40 Holly Lane Premises. A defendant can establish that he had a legitimate expectation of privacy with respect to a home sufficient to invoke Fourth Amendment rights “by showing that he owned the premises or that he occupied them and had dominion and control over them by leave of the owner.” *Watson*, 404 F.3d at 166 (quoting *Villegas*, 899 F.2d at 1333). It is not necessary that the defendant own the home or be a signatory on a lease or rental agreement; even an overnight guest can have a Fourth Amendment right when he resides at a home “with the permission of his host, who is willing to share his house and his privacy with his guest.” *Minnesota v. Olson*, 495 U.S. 91, 99 (1990); *see also United States v. Bullock*, 2010 WL 1948591, at \*17 (S.D.N.Y. May 13, 2010) (“[A]n overnight guest in someone else’s home has a cognizable Fourth Amendment interest”). However, in order to establish a Fourth Amendment right, the defendant must put forth some evidence that he “reside[d] at the subject premises at the time the warrant was executed.” *Watson*, 404 F.3d at

166. Although the defendant need not be physically present in the premises when the warrant is executed to assert a Fourth Amendment right, *Michigan v. Clifford*, 464 U.S. 287, 295 (1984) (holding that plaintiffs had a reasonable privacy interest in their home, even when they were not physically present), the defendant has no Fourth Amendment rights when, for example, he or she has abandoned the premises. *United States v. Levasseur*, 816 F.2d 37, 44 (2d Cir. 1987) (“ . . . one forfeits any reasonable expectation of privacy upon abandoning one’s property”); *United States v. Wyler*, 502 F. Supp. 959, 966 (S.D.N.Y. 1980) (“Once the initial proprietary interest is established the core question becomes whether the complainants have abandoned their reasonable expectations of privacy in the property searched or the goods seized. If the reasonable expectation of privacy has been abandoned, the defendants suffer no infringement of Fourth Amendment rights when the property is searched or goods are seized.”) (internal citations omitted).

Ray has said enough to satisfy the constitutional standard for establishing that he had a legitimate expectation of privacy that was implicated by the Government’s search. In his declaration, Ray states that he lived at the 40 Holly Lane Premises “[b]efore [he] was arrested and incarcerated.” Standing on its own, this statement could admit of the reading that Ray did not live at the 40 Holly Lane Premises at the time of the search and, if so read, might not be enough to establish a legitimate expectation of privacy at that time. However, the declaration submitted in connection with the motion to suppress the evidence seized from the 40 Holly Lane Premises cannot be read in isolation. In connection with another motion in this case, Ray submitted a declaration in which he swore under oath that when the agents arrived to conduct the search of the 40 Holly Lane Premises, he had been asleep at the location. Dkt. No. 109-1 ¶ 3. He described the 40 Holly Lane Premises as his “home” and the room in which he was

questioned as his “bedroom.” *Id.* ¶¶ 2, 5. In these circumstances, Ray had a legitimate expectation of privacy with respect to the 40 Holly Lane Premises.

Ray has not, however, established standing to challenge the search of the Storage Unit. Ray swears that he “kept a storage area in a locked facility at 140 West Ethel Road in Piscataway, New Jersey, which [he] expected to remain private.” Dkt. No. 160. As the Storage Unit Search Warrant Affidavit makes clear, the facility at 140 West Ethel Road is “an open plan storage facility,” with structural dividers. Dkt. No. 110-1 at 314. The Storage Unit which the warrant authorized the agents to search was limited to just one of the locked units at that location—Unit J. Unit J was the only location that was searched. Thus, Ray’s declaration is insufficient to establish that he had Fourth Amendment rights with respect to the premises the agents searched for two reasons. First, while the declaration reflects that Ray expected that some location within the 140 West Ethel Road facility would remain private, it steers clear from the claim that he had an interest in or control of or a reasonable expectation of privacy with respect to the particular storage unit within that facility that was the subject of the search and where the allegedly incriminating material was found and seized. An individual cannot establish standing to challenge the search of each apartment in a multi-apartment building by swearing that he resides in one of the apartments. *See, e.g., United States v. Shaw*, 269 F. Supp. 2d 90, 91 (E.D.N.Y. 2003) (“It is well-settled that individual tenants in multifamily dwellings have no legitimate privacy expectation in common areas, even when guarded by locked doors.”) (internal quotation marks and citations omitted). A person likewise does not acquire Fourth Amendment rights in all safety deposit boxes in a bank simply by possessing ownership rights with respect to one of those boxes. *See, e.g., United States v. Wetselaar*, 2013 WL 8206582, at \*14 n.12 (D. Nev. Dec. 31, 2013) (holding that a person owning a safe deposit box has a privacy interest only

in “the *contents* of the safe deposit box, not the box or the door itself, which is exposed to view by others who enter the . . . vault.”). It follows that an individual who has an interest in one storage unit in a multi-storage unit facility does not possess a privacy interest in all units in the facility. Ray’s sworn statement is insufficient to establish standing with respect to the Storage Unit that was the subject of the search.

Moreover, while Ray swears to his subjective expectation of privacy with respect to some storage area at the 140 West Ethel Road location, he fails to adduce any facts to support his contention that he had his expectation of privacy was legitimate or “one that society is prepared to recognize as ‘reasonable’ . . . whether, in the words of the *Katz* majority, the individual’s expectation, viewed objectively, is ‘justifiable’ under the circumstances.” *Smith v. Maryland*, 442 U.S. 735, 740 (1979) (quoting *Katz v. United States*, 389 U.S. 347, 361, 353 (1967)). It is not sufficient that Ray “kept” the storage area or that he stored his possessions in the storage area. A person does not acquire Fourth Amendment rights in another’s home by the simple expedient of keeping his possessions there. *United States v. Hollis*, 780 F.3d 1064, 1068 (11th Cir. 2015) (“[A] person has no greater right of privacy in another’s home than in his own.”) (quoting *United States v. Agnew*, 407 F.3d 193, 197 (3d Cir. 2005)). Ray must put forth some evidence that he had either a possessory interest in the storage area or was able to exercise some dominion or control over it. *See Watson*, 404 F.3d at 166. He has not done so.

#### **B. Omissions from the CSLII, Email, and iCloud Search Warrant Affidavits**

Ray also argues that evidence from the CSLI search and the searches of the email and iCloud accounts must be suppressed because the affidavits supporting those warrants omitted material information and thus were knowingly or recklessly false. In the alternative, he seeks a *Franks* hearing. Because Ray has established Fourth Amendment rights with respect to at least

one of the cellphones and seven of the email and iCloud accounts, the Court examines his arguments as to each of the search warrant affidavits. Based on that examination, the Court denies Ray’s motion to suppress and his request for a hearing.

1. The alleged omission of information from the CSLI Search Warrant Affidavit

Ray moves to suppress evidence seized pursuant to the CSLI Search Warrant on the grounds that the affidavits supporting those warrants omitted information regarding the credibility of FV-1 that would have undermined the showing of probable cause, had it been included. As noted above, the CSLI Search Warrant Affidavit relied on information from the Article which the Affidavit stated was corroborated by FV-1. The CSLI Search Warrant Affidavit stated that FV-1—who was not the source of the Article but had fact-checked it—“ha[d] been credible and corroborated in part by other evidence.” Dkt. No. 112-1 at 12. Ray complains that the CSLI Search Warrant Affidavit omitted evidence that called into question FV-1’s reliability as a witness, including that: (1) FV-1’s friends reported that she “stretched the truth for effect,” and “wanted to make herself more exciting,” and was the “best at [] telling stories”; (2) FV-1 wrote in a blog post that she would lie to her parents and her teachers; (3) in the same blog post, FV-1 described Ray as a “friend and a confidant,” and FV-1 told friends that Ray was a “good guy”; (4) FV-1 wrote in an email to the dean of Sarah Lawrence College stating that she “made false allegations to the police” about Mr. Ray; (5) in 2015, FV-1 testified under oath that she had poisoned Ray, lied to him and his daughter, and later became his friend; (6) FV-1 was arrested for prostitution and told police that she was not being trafficked and told at least one client the same thing. Dkt. No. 137 at 11. Ray argues that this information, which was omitted from the CSLI Search Warrant Affidavit, would have undermined FV-1’s statements and that without FV-1’s statements, there was insufficient probable cause for investigators to obtain

the historical cell site information. He thus argues that the search warrant for the cell site information must be voided and the fruits of the search excluded.

The argument lacks merit. As an initial matter, Ray fails to identify any material information omitted from the CSLI Search Warrant Affidavit. To determine whether the alleged misstatements or omissions are material, the Court must “disregard the allegedly false statements” and “insert the omitted truths” and, after doing so, “determine whether there remains a residue of independent and lawful information sufficient to support probable cause.” *Nejad*, 436 F. Supp. 3d at 719 (internal citations omitted). Where information is allegedly omitted, the question is whether the warrant, with the addition of the omitted information would still support probable cause. *See Franks*, 438 U.S. at 156; *United States v Canfield*, 212 F.3d 713, 718 (2d Cir. 2000). “If, after setting aside the allegedly misleading statements or omissions, the affidavit, nonetheless, presents sufficient information to support a finding of probable cause, the district court need not conduct a *Franks* hearing.” *Salameh*, 152 F.3d at 113; *see also Ganek*, 874 F.3d at 82 (“To determine whether a false statement was necessary to a finding of probable cause, [the court] consider[s] a hypothetical corrected affidavit, produced by deleting any alleged misstatements from the original warrant affidavit and adding to it any relevant omitted information.”). The CSLI Search Warrant Affidavit passes that test. The CSLI Search Warrant Affidavit contained detailed information that FV-1 provided directly to law enforcement. That information provided the probable cause necessary to support the CSLI Search Warrant. It included that Ray moved in with the Roommates; that FV-1 spent time with Ray at the 93<sup>rd</sup> Street residence and that Ray slept in the same room as Isabella Pollok, *id.* at 12; that Ray provided FV-1 with counseling sessions and provided some of the Roommates with sex education, *id.*; that Ray physically abused FV-1 and that she witnessed Ray hit Felicia Rosarios,

among others, *id.* at 13; that FV-1 traveled to Pinehurst, North Carolina, where she was forced to work in the backyard of Ray's stepfather without pay; that Ray shoved her and berated her for doing bad work in the yard, and on another occasion left her to sleep outside and deprived her of food for more than a day; that Ray hit her and other Roommates, and that Talia Ray, Pollok, and others were there, *id.* at 12-13; that FV-1 came to believe that she had in fact poisoned Ray and confessed to it at Ray's urging, including in a videotaped confession that was later posted on Youtube, *id.* at 12; that in or about 2014, at Ray's suggestion, FV-1 began working as an escort and that she gave the proceeds from her escorting to him after he suggested that by doing so she could repair the damage she had done, including the damage done by poisoning him; that Ray had strapped FV-1 to a chair and put a plastic bag over her head; and finally that in or about April 2019, after Ray spoke to FV-1 about the impending Article, she ran away with the aid of a former employer, *id.* at 14.

FV-1 was a percipient witness and victim who provided information directly to law enforcement. *See Caldarola v. Calabrese*, 298 F.3d 156, 165-66 (2d Cir. 2002) (“[I]t is well-established that a law enforcement official has probable cause to arrest if he received his information from some person, normally the putative victim or eyewitness, who it seems reasonable to believe is telling the truth”) (quoting *Miloslavsky v. AES Eng'g Soc.*, 808 F. Supp. 351, 355 (S.D.N.Y. 1992)), *aff'd*, 993 F.2d 1534 (2d Cir. 1993)); *United States v. Salazar*, 945 F.2d 47, 50-51 (2d Cir. 1991) (an informant is more reliable if he meets with the police face-to-face because he runs a greater risk that he will be held accountable if his information proves false). The information she conveyed would have been personally embarrassing to her and she had no apparent motive to curry favor with the police. *See United States v. Rollins*, 522 F.2d 160, 164 (2d Cir. 1975) (the report of an “identified bystander apparent motive to falsify” has a

“peculiar likelihood of accuracy”) (quoting *United States v. Miley*, 513 F.2d 1191, 1204 (2d Cir. 1975)).

The information that was allegedly omitted would not have cast FV-1 in a materially different light or raised issues about her credibility that were not already presented in the CSLI Search Warrant Affidavit. Much of that information dates to the time period from 2003 to 2014 and concerns statements that FV-1 made about Ray. That information does not undermine the showing of probable cause. The CSLI Search Warrant Affidavit makes clear that during that time period from 2003 to 2014, FV-1 was under the control of Ray and was induced by Ray to make statements that falsely exculpated Ray and falsely inculpated herself. The fact that FV-1 during that time period made favorable statements about Ray and accused herself of harming Ray would not have come as a surprise to the magistrate judge. The whole thrust of the affidavit was that, although FV-1 had made favorable statements about Ray and had confessed to harming Ray, she had done so at Ray’s behest and as part of a scheme by him to use the false confessions to extract forced labor and commercial sex acts.

Ray does identify statements about FV-1 from prior to the time she came under his influence that he claims cast doubt on her credibility. But those statements are not of the sort that would undermine confidence in FV-1’s statements to the FBI in the summer of 2019. Ray notes that FV-1’s friends told New York Magazine that, when she was a high school student, FV-1 had a reputation for “stretch[ing] the truth” and being a good storyteller. The statements dated from when FV-1 was a high school student and were entirely general in nature. The fact that a person had a reputation for stretching the truth while in high school does not raise meaningful doubts about that person’s credibility with respect to statements she made years later as an adult to law enforcement about a crime in which she participated but of which she was also



a victim. It does not suggest that as an adult FV-1 would lie or had lied about a matter of importance, nor does it cast doubt on the probable cause established by the warrant. *See, e.g., United States v. Fortes*, 619 F.2d 108, 118 (1st Cir. 1980) (“[T]he district court is not bound to allow examination into every incident, no matter how remote in time and circumstances, that may possibly bear upon the witness’ veracity.”); *United States v. Pickard*, 211 F. Supp. 2d 1287, 1295 (D. Kan. 2002) (“[A]n isolated untruth may have little, if any, conceivable relevance to a witness’ credibility.”). Significantly, Ray does not allege that FV-1 made any false statements after April 2019 when she refused to speak with him and instead ran away and thus ceased to be under his control, or indeed after 2018, when she was allegedly physically assaulted by Ray.

Moreover, FV-1’s reports to law enforcement cannot be viewed in isolation. The CSLI Search Warrant Affidavit also contained extensive independent evidence from the Article and from sources that corroborated the Article and FV-1 that alone went far in establishing probable cause. The Article itself was written by two “identified private” journalists writing for a magazine of high repute and of substantial reputation. It reported that Ray induced false confessions from his victims and posted at least one of them on YouTube; that he forced them to work in the backyard of his stepfather’s house in North Carolina by physically threatening and abusing them and depriving them of food and sleep; and that he encouraged them to work as escorts and compelled them to return all earned proceeds to him to pay for property damage they purportedly caused; and that on one occasion he tied FV-1 to a chair, placed a plastic bag over her head, and threatened to kill her. Dkt. No. 110-1 at 12-14.

The Article was not an anonymous blog post published without any editorial review and therefore entitled to little credibility or weight. Its veracity “is generally presumed in the absence of special circumstances suggesting that [the reporter] should not be trusted.” *See United States*

*v. Elmore*, 482 F.3d 172, 180 (2d Cir. 2007) (addressing reliance in a search warrant affidavit on a confidential informant); *see also id.* at 180 (noting that when an informant is identified his “reputation may be assessed and he may be held accountable if his allegations turn out to be fabricated”) (quoting *Florida v. J.L.*, 529 U.S. 226, 270 (2000)). Ray has identified no such special circumstances here. There is no reason to think that the reporters “concocted [a] story . . . in order to harass an innocent or [to] curry favor with the police.” *United States v. Wagner*, 989 F.2d 69, 73 (2d Cir. 1993). Nor is there evidence that the reporters were trying to curry favor with Ray’s putative victims or that they had a particular interest in falsely inculpating Ray or exculpating his victims. The reporters’ account was given, not in private to the police, but in public where it would be subject to scrutiny, to potential attack and response, and to the risk of a defamation suit if it were untrue. Moreover, the CSLI Search Warrant itself reflected that the reporters printed both sides of the story. The Article included not only the accounts from the putative victims but also Mr. Ray’s response.

Furthermore, although the reporters do not purport to be percipient witnesses or to have first-hand knowledge of the information contained in the Article, the “second-hand information” on its face comes from sources who did have first-hand knowledge and whom the magistrate judge was entitled to conclude were “reliable.” *Wagner*, 989 F.2d at 73. The Article indicates that several of the Roommates spoke with the reporters. Ray himself provided more than ten hours of interviews. The reports themselves would have been embarrassing to and potentially incriminating of the sources who provided the information, lending them additional credibility. The roommates who spoke to the reporter did not just make accusations against Ray; they also identified themselves as having been engaged in wrongful conduct. The Article indicated that Ray himself corroborated portions of the story, including that he was presently living in New

Jersey with two of the Roommates, that FV-1 was engaged in escorting, and that he had taken money from FV-1 to pay him back for the damage he says that she caused.

Ray seeks to downplay the Article as, at best, “akin to an anonymous tip” and, at worst, “unsubstantiated rumors.” Dkt. No. 112 at 43. *Gates* instructs, however, that there are no per se rules excluding certain sources of information from the probable cause analysis and that even “anonymous tips” from the most unsavory types, particularly when supported by corroborative police work, can establish probable cause. *See United States v. Fama*, 38 F. App’x 70, 72 (2d Cir. 2002); *see Gates*, 462 U.S. at 237-38 (holding that information from an anonymous source can be a basis for a finding of probable cause). There is no reason in principle or in the case law why the agents and the magistrate judge could not also rely on the information contained in the Article.

In addition, important parts of the Article were independently corroborated by the agents, even apart from the information from FV-1. The Article reported that Ray lived in an apartment on East 93<sup>rd</sup> Street in Manhattan, where he spent time with some of the Roommates. Dkt. No. 110-1 at 10. The agent’s review of records from GoDaddy corroborated that Ray used the 93<sup>rd</sup> Street residence as his address. *Id.* at 14. The Article reflected that Ray had a relationship with Isabella Pollok and that Pollok slept in the same room as Ray at the 93<sup>rd</sup> Street residence. The records from GoDaddy revealed that for certain domains names on GoDaddy registered to the name Lawrence Ray, the billing information provided listed Isabella Pollok’s name and the 93<sup>rd</sup> Street residence as the billing address. *Id.* at 15. The Article reported that FV-1 was engaged in work as an escort. *Id.* at 11. Paypal records revealed that FV-1 had an account into which she deposited proceeds from escort clients. *Id.* at 15. The article reported on communications among Ray, Pollok, and FV-1, including that Ray and Pollok demanded the escorting proceeds

from FV-1. Phone records from Verizon Wireless corroborated that Ray, Pollok, and FV-1 all knew one another and were in touch with one another. *Id.* at 14-15.

“All storytelling involves an element of selectivity,” *United States v. Vilar*, 2007 WL 1075041, at \*27 (S.D.N.Y. Apr. 4, 2007) (quoting *Wilson v. Russo*, 212 F.3d 781, 787 (3d Cir. 2000)), and a search warrant affidavit need not “include . . . every piece of information gathered in the course of an investigation.” *Awadallah*, 349 F.3d at 67-68. The CSLI Search Warrant Affidavit itself stated that it did not include all the facts SA Maguire learned during her investigation, because it was submitted for the limited purpose of obtaining the warrant. And while the CSLI Search Warrant reported SA Maguire’s view that FV-1 “has been credible and corroborated in part by other evidence,” Dkt. No. 110-1 at 12, that statement cannot be understood as a representation that FV-1 had never lied. The CSLI Search Warrant Affidavit reported that FV-1 had lied in the past at the behest of Ray. It reported statements FV-1 made after she was no longer under Ray’s influence and, as such, it is not undermined by the omitted information.

Finally, even if the information omitted from the CSLI Search Warrant Affidavit were material, Ray has made no showing—much less a substantial preliminary showing—that SA Maguire intentionally misrepresented the facts or “entertained serious doubts as to the truth of [her] allegations.” *Rajnaratnam*, 719 F.3d at 154 (quoting *United States v. Whitley*, 249 F.3d 614, 621 (7th Cir. 2001)). There is no evidence that the Government had the actual Housing Court testimony or FV-1’s emails and arrest records until the fall of 2019 when, according to the Government’s account “another witness in the case turned over a disc of the housing court testimony” and “the Government obtained a court-issued unsealing order . . . for FV-1’s arrest records.” Dkt. No. 118 at 63. There also is nothing in the blog post itself that would have

caused the agent to conclude that it would need to be disclosed. It contains precisely the types of confessions of hurting Ray and damaging his property that, according to the Affidavits, Ray was inducing FV-1 and the other Roommates to make at the time.

Ray argues that, even if the Government did not have the transcript, it should have known from the Article that FV-1 likely had made false statements to the Housing Court and in the email to the dean of the College. But if that is so, that would help defeat Ray's argument and would not support it. The agent did not hide the existence or location of the Article or conceal her reliance on it. She disclosed it prominently including its title, location, and date for anyone to check who wanted to do so. It thus was readily apparent, and available to, the issuing judge. The conduct is exactly the opposite of what one would expect from a party intentionally misrepresenting facts.

Ray additionally argues that some of occasions on which FV-1 allegedly lied occurred while she was not with him. Ray notes that he was not present at the 2015 Housing Court hearing, at which FV-1 testified that she had poisoned Ray and that she had pretended to have emotional problems and problems at home. Dkt. No. 110 at 29. She did not testify at the hearing that she was working as an escort or as a prostitute. *Id.* at 30. This argument ignores the contents of the affidavit. The fact that FV-1 allegedly lied outside of Ray's presence during the period when he allegedly controlled her does little to impugn her credibility. The Government's theory of the case is that Ray manipulated his victims with verbal and physical abuse in order to control their lives to enrich himself through sex trafficking and forced labor. The CSLI Search Warrant Affidavit reflected that after his release from prison Ray "began to control aspects of the lives of some of the Roommates," Dkt. No. 110-1 at 10, that Ray had asked FV-1 about her poisoning him to the point where she "started to believe that she had in fact poisoned Ray and

others,” *id.* at 12, and that the FBI was investigating Ray for “manipulating his victims with verbal and physical abuse, and grooming and coercing them to engage in conduct to enrich himself,” *id.* It also reported that, in the agent’s experience, “individuals who engage in sex trafficking often groom their victims for prostitution or escorting through verbal manipulation and physical and verbal abuse, as RAY engaged in here, including through the ‘counseling sessions,’ confessions, threats, and physical assault.” *Id.* at 14. The fact that FV-1 lied on Ray’s behalf in Housing Court is consistent with this theory, and thus does not meaningfully impact her credibility.

## 2. The alleged omissions from the Email and iCloud Search Warrant Affidavits

Ray’s argument that the Email and iCloud Search Warrant Affidavits excluded material information and his request for a *Franks* hearing with respect to those warrants also is without merit. Both the Email Search Warrant Affidavit and the iCloud Search Warrant Affidavit contained extensive information supporting the finding of probable cause. Specifically, they included information from third-party sources that corroborated the information from the Article and from FV-1, including advertisements promoting commercial sex acts with FV-1 that the FBI had located on Internet websites; financial records showing that FV-1 had received what appeared to be prostitution proceeds and had provided those proceeds to Ray or another co-conspirator; and records showing communications among the conspirators and with the Roommates. *See Wagner*, 989 F.2d at 73 (“If a substantial amount of information from an informant is shown to be reliable because of independent corroboration, then it is a permissible inference that the informant is reliable and that therefore other information that he provides, though uncorroborated, is also reliable.”). The addition of the information from the New York City Housing Court and the email to the dean of Sarah Lawrence would not have done anything

to undermine the showing of probable cause. It likely would only have enhanced it. As already noted, that information would tend to have provided additional examples of FV-1 making false statements while under the control of Ray. It was not contrary to the evidence proffered to support probable cause but was of a piece with it.

Moreover, far from concealing the email to the dean of the College or intentionally misrepresenting it, the Email and iCloud Search Warrant Affidavit referred to and described it. It noted that FV-1 “had sent an email to the dean of the College stating that, although she had previously expressed concerns about Ray, including that he was a bad, dangerous, manipulative, and sexually deviant person, those concerns had been unfounded, and Female Victim-1 had been tricked into expressing them by Ray’s ex-wife.” Dkt. No. 118 at 86. Those affidavits also contained FV-1’s admission that at the time she was introduced to Ray, “[s]he was using illegal drugs, suffered from insomnia, and was struggling with other personal issues, including interpersonal problems with her parents,” *id.* at 89, as well as FV-1’s statement that she had made many false confessions, as had others, and that she had lied to her escorting and prostitution clients, due to Ray’s pressure. *Id.* at 92-94. Finally, they contained a cite to the Article, which also contained information Ray alleges the agents intentionally concealed. In this light, the “alleged deficiencies [are] too insignificant to suggest that [the agent] had deliberately falsified information or shown a reckless disregard for the truth.” *Levasseur*, 816 F.2d at 43.

### **C. Ray’s Challenge to the Premises Search Warrant and the Storage Unit Search Warrant as Overbroad and Unparticularized**

Ray challenges both the Premises Search Warrant and the Storage Unit Search Warrant as overbroad and unparticularized. He argues that several of the categories of items to be seized were not qualified by the language “related to the subject offense”—permitting the agents to

seize documents “without limitation,” Dkt. No. 112 at 40, and that even where categories of evidence authorized to be seized were qualified as limited to those “related to the subject offense,” such language was “incantatory” and “repetitive” and not sufficient to provide guidance to allow the executing agents to determine what records to seize. *Id.* at 40-41. He notes that while the warrants authorized the agents to seize documents “related to the subject offenses,” they “provided no key words, no names, no identifying descriptions of specific items.” *Id.* at 41. The result, he contends, was “the seizure of a massive number of unresponsive documents.” *Id.* at 41. He also argues that in the execution of the warrant, the Government seized documents unresponsive to the categories of materials the Government was authorized to seize under the express terms of the warrant and seeks a hearing related to the Government’s search protocols. Dkt. No. 137 at 15-19. The Court first considers Ray’s challenge to the particularity of the warrant with respect to items other than electronic devices. It then turns to the particularity of the permission to seize electronic devices. Finally, it addresses the execution of the warrant and the request for a hearing. The Court concludes both that Ray has failed to establish that the warrants were invalid and that even if the warrants were invalid in some respect, law enforcement relied in good faith on them, precluding the remedy of suppression. The motion to suppress and the request for a hearing are denied.

#### 1. The particularity of the Premises Search Warrant

Ray’s challenge to the Premises Search Warrant is without merit. The Premises Search Warrant identifies with particularity the items to be seized and ties those items to the crimes as to which the Premises Search Warrant Affidavit provides probable cause. In certain instances, the face of the warrant limits the agents to seize items only if they are related to the Subject Offenses. Those items include: books and records related to the Subject Offenses; evidence



concerning the identity or location of, and communications with participants and co-conspirators in the Subject Offenses; financial records related to the Subject Offenses; proceeds of the Subject Offenses; and communications related to the Subject Offenses. There can be no particularity challenge to those items. Each links the evidence to the criminal activity supported by probable cause. The agents did not have authority to seize all financial records or all communications but only those related to the Subject Offenses. *Ulbricht*, 858 F.3d at 99.

Ray argues that the Premises Search Warrant Affidavit does not define with sufficient particularity items such as financial records related to the Subject Offenses. He notes that the warrant left it to the agent's judgment which financial records would be related to the Subject Offenses. However, the Fourth Amendment does not require law enforcement agents or the issuing magistrate to anticipate in advance the precise financial records they will find or are permitted to take with greater specificity. *See United States v. Regan*, 706 F. Supp. 1102, 1113 (S.D.N.Y. 1989) (holding that less specificity is required "in cases involving complex schemes spanning many years that can be uncovered only by exacting scrutiny of intricate financial records.") (quoting *United States v. Christine*, 687 F.2d 749, 760 (3d Cir. 1982)). Some judgment must be left to the agent acting on the spot. "[U]nlike other forms of property, business records are often incapable of being itemized one-by-one." *United States v. Cohan*, 628 F. Supp. 2d 355, 360 (E.D.N.Y. 2009) (quoting *United States v. Zanche*, 541 F. Supp. 207, 210 (W.D.N.Y. 1982)). Whether a particular financial record related to the Subject Offenses or not could not have been determined in advance—a record might or might not be related. It would only be by viewing it that the agent would know. The charged scheme was "complex," lasted many years and involved many different alleged victims. Accordingly, its "existence could be proved only by piecing together many bits of evidence," [unlike] a straightforward crime such as

drug possession where the types of evidence that will be relevant are few and obvious.” *Id.* (quoting *Andresen v. Maryland*, 427 U.S. 463, 482 n.10 (1976)). The warrant description enabled “the executing officer to ascertain and identify with reasonable certainty those items that the magistrate has authorized [her] to seize.” *United States v. George*, 975 F.2d 72, 75 (2d Cir. 1992).

The warrant did not give the agents broad authority to search for all evidence of the Subject Offenses without any limitation. *Cf. United States v. Buck*, 813 F.2d 588, 590 (2d Cir. 1987) (holding that warrant authorizing agents to search and seize “any papers, things or property of any kind relating to previously described crime” was not permissible under the Fourth Amendment but affirming denial of motion to suppress because agents relied on warrant in good faith). It limited the agents’ authority to financial records and the other specifically defined items. *See id.* at 591 (indicating that even a warrant that contains broad, boilerplate language will be upheld if “preceded by a list of specific items to be sought by the police”). Thus, it is enough that, as the Premises Search Warrant Affidavit establishes, there was probable cause to believe that the financial records would be probative of the Subject Offenses and that the warrant limited the agents to seizing only those financial records that related to the Subject Offenses. The court need not have delineated, nor need the agents have anticipated in advance, exactly what records they would find that would relate to the Subject Offenses.

Ray focuses on the items in the Premises Search Warrant that are not limited on their face as being “related to the Subject Offenses.” The Premises Search Warrant authorized the agents to seize, for example, “[a]address and/or telephone books, any pagers, or cellphones that . . . have the ability to store names, addresses, telephone numbers, page numbers, fax numbers of co-conspirators, victims, and clients”; “[e]lectronic devices”; “records that refer or relate to the

receipt, origin, disbursement or concealment of money and property”; and “backpacks and their contents.” Dkt. No. 110-1 at 246-47; Dkt. No. 137 at 12. None of these categories of items were qualified by the requirement that they be “related to the Subject Offenses.” Ray argues that, without the limiter “related to the Subject Offenses,” the Premises Search Warrant failed to limit the agents to items that would be evidence, proceeds or instrumentalities of the Subject Offenses.

However, each of the items Ray challenges were themselves evidence or instrumentalities or the fruits of the Subject Offenses. No further limitation was necessary. For example, the address books and telephone books and pagers that the Premises Search Warrant gave the agents authority to seize were both evidence and instrumentalities of the Subject Offenses. The Premises Search Warrant Affidavit established that Ray communicated with those who joined in his criminal activity or who were its victims by phone and email. It thus was relevant and permissible for the agents to seize a telephone book or address book. Those items were the means by which Ray allegedly committed his crimes. They also could tie Ray to the other alleged participants and to the victims and thus would be corroborative of the criminal conduct for which the Premises Search Warrant Affidavit provided probable cause.

Likewise, while the Premises Search Warrant gave the agents broad authority to seize all records related to the receipt or disbursement of money, the Premises Search Warrant Affidavit provided probable cause that Ray received cash proceeds from the commission of the Subject Offenses and engaged in money laundering with respect to such proceeds. All records related to the receipt and disbursement of money were directly relevant to, and likely to be evidence of, the Subject Offenses without the need for further limitation.

The Premises Search Warrant also allowed the agent to seize “[b]ackpacks and their contents,” but the Premises Search Warrant Affidavit laid out evidence from one victim that Ray carried a backpack on his person at all times, in which he maintained large sums of cash. Dkt. No. 110-1 at 267. The backpack itself was thus both evidence of the Subject Offenses and an instrumentality used to commit them. The agent described videos she reviewed showing Ray wearing a backpack with a padlocked zipper. *Id.* She also laid out evidence that Ray and an associate collected cash proceeds from FV-1 that she earned escorting, and that cash deposits were made to the accounts of others of the Roommates. For that reason, the permission to seize backpacks and their contents was “justified” and no “broader” than necessary based on the probable cause upon which the warrant is based.” *Galpin*, 720 F.3d at 446. The backpack itself was used by Ray in his commission of the crimes for which the warrant established probable cause. It also had evidentiary value, corroborating the relevant testimony of a witness that Ray carried a backpack and used it in the commission of the offenses, to collect cash from and dispense it to his victims.

Ray argues that the Premises Search Warrant broadly gives the agents authority to seize all “electronic devices” and “all cellphones.” Dkt. No. 137 at 12. Where the property to be searched is a hard drive or other electronic media, “the particularity requirement assumes even greater importance,” *Ulbricht*, 858 F.3d at 99 (quoting *Galpin*, 720 F.3d at 446), for “[t]he ‘seizure of a computer hard drive, and its subsequent retention by the government, can . . . give the government possession of a vast trove of personal information about the person to whom the drive belongs, much of which may be entirely irrelevant to the criminal investigation that led to the seizure.’” *Id.* (quoting *United States v. Ganius*, 824 F.3d 199, 217 (2d Cir. 2016)). But here, the Premises Search Warrant Affidavit supplied probable cause to believe that electronic devices

and cellphones were used to communicate to cohorts, ensnare victims, and generally to prepare and orchestrate criminal conduct.” *Vilar*, 2007 WL 1075041 at \*36. It also identified the items to be searched and seized and linked them to the suspected criminal activity—the Subject Offenses. *See* Dkt. No. 110-1 at 254 (“Following the seizure of any computer devices and storage media and/or the creation of forensic image copies, law enforcement personnel . . . will review the ESI contained therein for information responsive to the warrant.”); *see also United States v. Guobadia*, 2021 WL 1811743 (2d Cir. May 6, 2021) (holding that a warrant “which specifically lists ‘computers and computer equipment (card scanners and embossers, printers)’ among the items to be seized can hardly be said to lack particularity”) (internal citation omitted); *cf. United States v. Rosa*, 626 F.3d 56, 62 (2d Cir. 2010) (search warrant did not comply with the particularity requirement where “the warrant directed officers to seize and search certain electronic devices, but provided them no guidance as to the type of evidence sought”). Agent Maguire averred that “Ray used electronic devices in the commission of the Subject Offenses, including to take and maintain explicit photographs and ‘confession videos,’” and that evidence of those offenses was therefore likely to be found on electronic devices within the premises. Dkt. No. 110-1 at 268. That statement was based on the accounts of some of the victims and was corroborated by the agent’s review of emails. *Id.* at 269. She also swore, based on her review of evidence, that cellphones recovered from the premises were likely to contain evidence of the Subject Offenses, such as text messages including photographs of written “confessions” and information regarding when FV-1 was seeing clients. *Id.* at 270-71. The affidavit did not rely simply on general allegations that files can be stored for a long time and can be recovered after deletion. *See United States v. Weigand*, 2020 WL 5105481, at \*10 (S.D.N.Y. Aug. 31, 2020). It contained specific examples of communications indicating that Ray was storing false confessions

from as recently as March 21, 2016. Dkt. No. 110-1 at 14. Agent Maguire also swore that it was likely that there would be laptop and desktop computers inside the premises; she had seen “multiple videos of . . . Ray using laptop and desktop computers” inside the Premises. *Id.* at 273. Agent Maguire also set forth her understanding, based upon her training and experience, that individuals who engage in extortion frequently maintain leverage materials, such as the recordings of false “confessions,” for years to frighten and intimidate victims, that where computers and electronic devices are used in furtherance of criminal activity, evidence of the criminal activity can often be found months or even years after it occurred, and that email and iCloud accounts are not device specific. *Id.* at 271. Thus, the Premises Search Warrant linked the request to seize electronic devices to the criminal activity for which it established probable cause and “designate[d] the information to be seized in connection with the specified offenses.” *Ulbricht*, 758 F.3d at 100.

This case is easily distinguishable from *United States v. Wey*, 256 F. Supp.3d 355 (S.D.N.Y. 2017), the primary case relied upon by Ray. The warrants at issue there had several distinctive characteristics. First, “on their face, both Warrants fail[ed] to set forth the crimes under investigation. . . . [T]hey neither cite[d] criminal statutes nor in any way describe[d] any criminal conduct.” *Id.* at 384. Second, the warrants had a circular structure that literally authorized the agents to seize every item within each of the subject premises regardless of its relation to the suspected criminal activity. The warrants each listed broad categories of items to be seized limited only by the qualifier that they relate to the individuals and entities listed on an exhibit to the warrants. In turn, the exhibit listed “among its first few entries the very corporate entity . . . whose premises was the subject of the first Warrant and Search and those very individuals . . . whose residence was the subject of the second. The result of that circular

structure is that the would-be constraint imposed by Exhibit B is no constraint at all.” *Id.* at 386. The warrant, in effect, authorized the agents to seize all items related to the owner of the premises. The court concluded that “the Warrants [we]re—in function if not in form—general warrants. Indeed, insofar as any document located within a home or office at least arguably pertains in some way to the occupant or owner of the premises, the Court would struggle to conceive of any documents found within NYGG or the Wey Apartment that would *not* colorably fall within the scope of authorization” *Id.* at 386. The court held that the warrants failed the Fourth Amendment particularity requirement because “[i]n sum, the Warrants authorize[d] the seizure of sweeping categories of materials, regardless of their potential connection (or lack thereof) to any suspected criminal activities and limited only by the requirement that they relate in some generalized way to the owner/occupant of the very premises subject to search” and “[t]he conferral of such unfettered discretion on the executing officers, particularly in light of the Warrants’ independent failure to identify any crime under investigation, [was] inconsistent with the Fourth Amendment’s particularity requirement.” *Id.* at 387.

## 2. The permission to search electronic devices

Ray also challenges the Premises Search Warrant Affidavit because it permitted the agents to seize electronic devices to be reviewed outside the location of the Subject Premises and on the theory that it provided no meaningful parameters for the agents’ review of the contents of the electronic devices.

Under Federal Rule of Criminal Procedure 41(e)(2)(B), a warrant may “authorize the seizure of electronic storage media or the seizure or copying of electronically stored information” and “[u]nless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant.” Fed. R. Crim. P. 41(e)(2)(B). Indeed, “due

to the unique challenges that electronic searches pose, ‘it is frequently the case with computers that the normal sequence of ‘search’ and then selective ‘seizure’ is turned on its head, as computer hardware is seized from a suspect’s premises before its content is known and then searched at a later time.” *Nejad*, 436 F. Supp. 3d at 728 (quoting *Vilar*, 2007 WL 1075041, at \*35); *see also United States v. Hill*, 459 F.3d 966, 974 (9th Cir. 2006) (finding that officers were permitted to remove computer and storage media from the defendant’s home pursuant to a search warrant “without first determining whether they actually contained child pornography”).

Thus, once the Government established probable cause to the satisfaction of the magistrate that electronic media at the 40 Holly Lane Premises would likely contain evidence, fruits, or instrumentalities of the subject offenses, the magistrate was authorized to permit the Government to seize the electronic media for later review at FBI headquarters. A contrary conclusion would be perverse. It would either preclude the agents from seizing the media at all or, more likely, require them to remain at the premises being searched while they methodically reviewed each of the items of electronic media, effecting an even greater intrusion on the occupant’s privacy.

Ray’s further argument that the warrant was defective for failure to provide a specific search protocol and for failure to provide meaningful parameters has no greater merit. “[O]utside the computer context, the Supreme Court has held that ‘it is generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized by warrant.’” *Vilar*, 2007 WL 1075041, at \*37 (quoting *Dalia v. United States*, 441 U.S. 238, 257 (1979)). As a general matter, the rule is no different when the search is to be conducted in the virtual or electronic world than in the physical world. “[T]he warrant need not specify *how* the computers will be searched.” *Id.* It need only require the Government to “reasonably limit its initial search, taking only those steps reasonably



necessary to identify documents responsive to the warrant.” *Weigand*, 2020 WL 5105481, at \*10.

Thus, Ray’s argument that the warrant should have required the agents to use specific search terms or keywords in their search finds no support in the law of this Circuit. “The reason for not imposing such a requirement on law enforcement in conjunction with search warrant applications for computer searches is obvious—in most instances, there is no way for law enforcement or the courts to know in advance how a criminal may label or code his computer files and/or documents which contain evidence of criminal activities. In other words, to require courts in advance to restrict the computer search in every case to certain methodologies or terms would give criminals the ability to evade law enforcement scrutiny simply by utilizing coded terms in their files or documents.” *United States v. Graziano*, 558 F. Supp. 2d 304, 315 (E.D.N.Y. 2008). However, “few people keep documents of their criminal transactions in a folder marked ‘drug records.’” *Weigand*, 2020 WL 5105481, at \*9 (quoting *United States v. Riley*, 906 F.2d 841, 845 (2d Cir. 1990)). As the Second Circuit has stated, “it will often be impossible to identify in advance the words or phrases that will separate relevant files or documents before the search takes place, because officers cannot readily anticipate how a suspect will store information related to the charged crimes. Files and documents can easily be given misleading or coded names, and words that might be expected to occur in pertinent documents can be encrypted; even very simple codes can defeat a pre-planned word search.” *Ulbricht*, 858 F.3d at 102. The warrant here specified all that was required in instructing the Government to limit its initial search only to those steps reasonably necessary to identify documents responsive to the warrant.

The Premises Search Warrant provided “meaningful parameters” on the permissible search and “identified with particularity” the underlying information to be seized. *Vilar*, 2007 WL 1075041, at \*36; *see also Graziano*, 558 F. Supp. 2d at 316 (“the government must show that there is probable cause that the computer will contain evidence of a crime and then state with reasonable particularity the materials to be seized”). The warrant did not permit the agents to take whatever they wanted from Ray’s computers regardless of its relevance to the Subject Offenses. The Premises Search Warrant limited the information permitted to be seized to that which was “responsive to the warrant” and which constituted “evidence or fruits of the Subject Offenses”. Dkt. No. 110-1 at 279. The Premises Search Warrant Affidavit contains the Government’s representation that it would “make reasonable efforts to restrict [its] search to data falling within the categories of evidence specified in the warrant for the time period 2010 to Present.” *Id.* at 280.

The Fourth Amendment does not prohibit law enforcement from seizing, pursuant to a warrant, electronic devices that are likely to contain evidence of crime simply because that evidence is likely intermingled with other non-criminal and private information. “[I]t is precisely because computer files can be intermingled and encrypted that the computer is a useful criminal tool.” *Vilar*, 2007 WL 1075041, at \*36. “[S]earches of computers may sometimes need to be as broad as searches of residences pursuant to warrants” and like searches for papers records, “searches for electronic records [may] entail[] the exposure of records that are not the objects of the search to at least superficial examination in order to identify and seize those records that are.” *Ulbricht*, 858 F.3d at 100. Nor does the Fourth Amendment require law enforcement to identify specific devices that it has evidence would contain evidence of crime at the cost of ignoring other devices that are likely to have such evidence or—if it cannot identify a

specific device—at the cost of ignoring all devices. *See Weigand*, 2020 WL 5105481, at \*10.

Thus, “law enforcement agents [did] the best that could reasonably be expected under the circumstances, [had] acquired all the descriptive facts which a reasonable investigation could be expected to cover and [had] insured that all those facts were included in the warrant.” *Ulbricht*, 758 F.3d at 100 (quoting *Galpin*, 720 F.3d at 446).

3. The agents relied in good faith on the warrant

Even if there were some defect in the language of the Premises Search Warrant Affidavit, it would not follow that suppression is the appropriate remedy. The Court would have to find that a “reasonably well-trained officer should have known that [the judge’s] warrant was impermissibly broad.” *Buck*, 813 F.2d at 592. There is no evidence before the Court to support that conclusion. The record shows that the agent presented the evidence supporting probable cause to a “neutral magistrate,” that the agent “outlined the crime for the magistrate,” and that the agent was placed under oath by the magistrate and swore to the truth of her allegations. *Id.* The agents complied with the terms of the warrant and those same terms were included in numerous cases in this Court approving search warrants for electronic devices and financial records. *See supra*. The Premises Search Warrant Affidavit on its face identified the Subject Offenses, contained a detailed list of the items to be searched, and limited the agents to searching for evidence, fruits and instrumentalities of the Subject Offenses. If, contrary to the Court’s holding above, the search warrants were impermissible, the only error of the officers would be to have failed to anticipate that holding. *See Buck*, 813 F.2d at 592; *see also Rosa*, 626 F.3d at 66 (holding that exclusionary rule would not apply where warrant was facially deficient because “[n]ot every facially deficient warrant . . . will be so defective that an officer will lack a reasonable basis for relying upon it” and the officers’ conduct was not “sufficiently deliberate

that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system”) (quoting *Herring v. United States*, 555 U.S. 135, 144 (2009)).

4. The execution of the warrant with respect to electronic devices and the request for a hearing

Ray argues that a hearing is necessary because the search of the devices went beyond what would be conducted had the agents limited themselves to a key word search and because “numerous materials unresponsive to the warrant were searched and seized by the government, including privileged documents.” Dkt No. 160 at 2-3. Those arguments fail to raise “contested issues of fact going to the validity of the search” that would require a hearing. *United States v. Watson*, 404 F.3d 163, 167 (2d Cir. 2005) (internal citations and quotations omitted). As to the fact that the agents went beyond conducting a key word search to a more fulsome (or less constrained) search, no hearing is necessary. That fact is undisputed; the warrant authorized the search to be conducted in that manner, the law in the Second Circuit permitted the magistrate judge to sign the warrant, and, in any event, the executing officers relied in good faith on the warrant. The Court need not hold a hearing to establish that the agents did what the Government said that they did.

Ray’s second argument is that the agents seized more than what the warrants gave them authority to seize. To the extent, however, that Ray relies on the quantity of information seized that argument does not necessarily establish anything more than that Ray and his co-conspirators used electronic devices extensively in the commission of the Subject Offenses and that those devices contained extensive evidence of the Subject Offenses. The amount of information seized cannot itself establish that the seized information went beyond that permitted by the warrant.

“[I]n many cases, the volume of records subject to seizure because of their evidentiary value may be vast. None of these consequences necessarily turns a search warrant into a prohibited general warrant.” *Ulbricht*, 858 F.3d at 98.

Ray’s argument is not furthered by the specific examples he cites of items that purportedly had nothing to do with the Subject Offenses. He complains that the Government seized notebooks that had nothing to do with the Subject Offenses, but those notebooks contain handwritten confessions of FV-1 and thus are evidence of the Subject Offenses. Dkt No. 115 at 48. He complains that the Government seized “handwritten recipes” and “drawings,” but those items were drawn by one of the alleged victims and thus also are evidence. *Id.* He complains that the Government seized information in Defendant’s possession yet pertaining to the victims, but the Premises Search Warrant Affidavit provided probable cause that such items would be evidence of the commission of the Subject Offenses which involved befriending the alleged victims and then using the information the victims conveyed to him to force them to engage in labor or commercial sex acts. *Id.*<sup>1</sup>

In short, the defense has offered the Court “no reason to doubt that the officers faithfully executed the warrant.” *Ulbricht*, 958 F.3d at 103. Accordingly, the motion to suppress and for a hearing is denied.

#### **D. Ray’s Challenge to the CSLI Search Warrant as Overbroad**

Ray argues that the CSLI Search Warrant “allowed a search of six years of location data, despite providing probable cause related to only two specific time periods and locations.” Dkt. No. 112 at 50. Ray argues that, “[a]t best, . . . the affidavit adequately alleges a nexus between

---

<sup>1</sup> Ray makes reference to the seizure of privileged information but does not identify any impropriety in the Government’s taint review.

the asserted probable cause and the information sought for only two time periods: October 15, 2018, when an assault allegedly occurred at a particular hotel, and for ‘six weeks’ around Father’s Day in 2013, when the forced labor charges allegedly occurred in North Carolina.” *Id.* at 51. In Ray’s view, the CSLI Search Warrant Affidavit did not create a sufficient nexus between the information sought and any probable cause asserted. Dkt. No. 110 at 50. He argues that it should have been limited to information about location on October 15, 2018 and for six weeks in 2013.

As an initial matter, to the extent Ray challenges the CSLI Warrant for permitting law enforcement to obtain evidence for the period prior to July 2018, there is nothing to suppress. Ray has standing only with respect to the 9122 cellphone and law enforcement received data with respect to that cellphone only for the period July 29, 2018 through July 26, 2019.

Moreover, Ray’s selective reading of the CSLI Search Warrant Affidavit fails to address the totality of the circumstances set forth in that affidavit, which supports a finding of probable cause with respect to the more extensive period of time. The evidence in the CSLI Search Warrant Affidavit was not limited to crimes committed for a few weeks in 2013 and on a single day in 2018. It laid out a complex course of criminal conduct that extended over years. *See Nejad*, 436 F. Supp. 3d at 729 (“[C]ourts in this Circuit have recognized that ‘[t]he complexity and duration of the alleged criminal activities’ may ‘render a time frame less significant than in a case that required a search for a small set of discrete items related to one or only a few dates.’”) (quoting *United States v. Hernandez*, 2010 WL 26544, at \*11 (S.D.N.Y. Jan. 6, 2010)). Thus, the specific events identified in the CSLI Search Warrant Affidavit had probative value that extended beyond the particular dates on which those events occurred; instead, they provided support for the theory that Ray was engaged in a criminal course of conduct involving a

particular set of victims that began prior to 2013 and that extended through and beyond October 2018. The CSLI Search Warrant Affidavit included information tending to show that Ray's unlawful conduct began shortly after his 2010 release from prison, when he moved in with his daughter and the Roommates in September 2010 and "began to control aspects of the lives of some of the Roommates." Dkt. No. 110-1 at 10. The CSLI Search Warrant Affidavit also contained averments that Ray extracted false confessions from FV-1 as early as 2014; that Ray routinely threatened to turn FV-1 in to the police for poisoning him; and that FV-1 began working as an escort in order to pay for the damage she had done to Ray's property in the same year. *Id.* at 11. It also contained the allegations that Ray and Pollok pressured FV-1 to see more clients and to charge higher prices in order to repay Ray for the damage FV-1 had purported caused. *Id.* at 13. The attack on FV-1 in October 2018 was thus no isolated incident, but was part of an extensive course of allegedly illegal conduct. Accordingly, there was no requirement that CSLI Search Warrant be limited to the period around Father's Day 2013 and the period after July 2018.

Finally, the search of the CSLI falls within the "good faith" exception to the exclusionary rule and thus suppression would not be the appropriate remedy even if the facts set forth in the CSLI Search Warrant Affidavit did not support probable cause for the full period set forth in the warrant. There is no dispute that the agent presented her evidence to a neutral magistrate who was exercising his judicial role and that the magistrate made the determination that the evidence supported probable cause. This is not a case where probable cause was so lacking that reliance on the warrant would be unreasonable, *see Clark*, 638 F.3d at 100, nor is the warrant so "facially deficient that reliance upon it [would be] unreasonable," *id.* (quoting *United States v. Moore*, 968 F.2d 216, 222 (2d Cir. 1992)). Thus, the motion to suppress on these grounds is denied.

**E. Ray's Challenge to the Email and iCloud Search Warrants as Being Overbroad and Unparticularized**

Ray's challenges to the Email and iCloud Search Warrants are similar to his challenges to portions of the Premises Search Warrant and fail for similar reasons. He argues that the two warrants were overbroad and unparticularized because they authorized the Government to search the entirety of the email and iCloud accounts when it had probable cause only to search a particular portion of the accounts. Ray complains that the Email Search Warrant used "broad catch-all phrase[s]" to obtain email information (including emails, email drafts, contacts and email attachments) spanning eight and a half years when "the affidavit notes with specificity emails between particular parties that are connected to the asserted probable cause." Dkt. No. 112 at 44. Ray argues, for example, that the warrant permitted the Government to seize all of Ray's correspondence with certain family members within the specified time periods, when the affidavit only referenced communications with those family members in shorter periods of time. *Id.* at 45. He also complains that "there was no limit in how the government could review the information," which he believes rendered the warrant overbroad. *Id.*

Ray similarly argues that the iCloud Search Warrant was overbroad and unparticularized. Ray says that the iCloud Search Warrant used "broad catch-all phrases" to seek categories of information including all emails associated with the account, all instant messages, all files and other records, all activity, and all information regarding locations. *Id.* at 46. Ray also takes issue with the fact that only the first two of those categories of data to be searched—emails and instant messages—had temporal limitations. *Id.* The iCloud Search Warrant also listed a narrower subset of information to "be seized by the government," which included communications about the Subject Offenses; photos and videos connecting Ray to the co-conspirators and victims;



evidence about the timing and manner in which the account was used; evidence “indicating the subscriber’s state of mind”; and any evidence that “may identify any co-conspirators.” *Id.* (internal citations omitted).

As previously mentioned, in order to satisfy the Fourth Amendment’s particularity requirement, a warrant must (1) “identify the specific offense for which the police have established probable cause”; (2) “describe the place to be searched”; and (3) “specify the items to be seized by their relation to the designated crimes.” *Ulbricht*, 858 F.3d at 99 (quoting *Galpin*, 720 F.3d at 445-46). “Search warrants covering digital data may contain ‘some ambiguity . . . so long as law enforcement agents have done the best that could reasonably be expected under the circumstances, have acquired all the descriptive facts which a reasonable investigation could be expected to cover, and have insured that all those facts were included in the warrant.’” *Id.* at 100 (quoting *Galpin*, 720 F.3d at 446)). A warrant also must be limited in its breadth such that the seizure does not include items “broader than can be justified by the probable cause upon which the warrant is based.” *Galpin*, 720 F.3d at 446 (quoting 2 W. LaFare, *Search and Seizure* § 4.61(a) (5th ed. 2012)). Breadth and particularity are “related but distinct concepts.” *Ulbricht*, 858 F. 3d at 102. Although a lack of particularity can result in a warrant’s overbreadth, a broad warrant does not necessarily lack particularity. *See Nejad*, 436 F. Supp. 3d at 729. To determine whether a warrant is overbroad, courts look to “whether there exists probable cause to support the breadth of the search that was authorized.” *Id.* (quoting *United States v. Zemlyansky*, 945 F. Supp. 2d 438, 464 (S.D.N.Y. 2013)).

The Email and iCloud Warrants met each of these requirements. To meet the first requirement, the Email and iCloud Search Warrant Affidavits identified the Subject Offenses and provided probable cause for each of them. *See supra* at 6-11. To meet the second requirement,

the Email and iCloud Search Warrants identified the email and iCloud accounts to be searched. *Id.* To meet the third requirement, the Email and iCloud Warrants linked the information to be seized to the Subject Offenses by offering ample reason to believe that each of the categories of information sought would be evidence or instrumentalities of at least one, if not all, of the Subject Offenses. *Id.* For example, the iCloud Search Warrant authorized seizure of evidence such as communications about the Subject Offenses; photos and videos connecting Ray to the co-conspirators and victims; and any evidence that “may identify any co-conspirators.” Dkt. No. 110-1 at 162-64. Those categories satisfy the third requirement of *Ulbricht* by “specify[ing] the items to be seized by their relation to the designated crimes.” *Ulbricht*, 858 F.3d at 99 (quoting *Galpin*, 720 F.3d at 446).

The two cases upon which Ray relies for his particularity argument, *Rosa* and *George*, are off point. The warrants at issue in *George* and *Rosa* authorized seizures without specifying the alleged legal violations. In *Rosa*, the search warrant did not meet the particularity requirements and constituted a general warrant because it authorized seizure of electronic equipment without specifying the legal violation, thereby “provid[ing] [officers] with no guidance as to the type of evidence sought.” *Rosa*, 626 F.3d at 62. Similarly, in *George*, the court found that the warrant lacked particularity because “mere reference to ‘evidence’ of . . . general criminal activity provides no readily ascertainable guidelines for the executing officers as to what items to seize.” *George*, 975 F.2d at 76. The warrants here specified the subject crimes and linked those crimes to the evidence of probable cause in the search warrant affidavits.

Ray argues that the Email and iCloud Search Warrants lack particularity because they allow for a “cursory inspection of all emails,” rather than a targeted review of only the specific communications referenced in the warrants and supported by probable cause. Dkt. No. 112 at

45. Ray bases his argument on a limited number of cases from other circuits and districts which have required that digital searches be particularized by using terms or specific time frames. *See Matter of Search Info. Associated with Four Redacted Gmail Accounts*, 371 F. Supp. 3d 843, 845 (D. Or. 2018) (finding that Google was capable of producing smaller subsets of emails in an account); *United States v. Blake*, 868 F.3d 960, 973 (11th Cir. 2017)).

Courts in this Circuit, however, have uniformly held that law enforcement need not rely upon an email host company or any other private party to sift through emails to determine what is relevant and that it may obtain a warrant to request all emails from an account. *See United States v. Redzepagic*, 2020 WL 5232066, at \*7-10 (S.D.N.Y. Sep. 2, 2020); *Nejad*, 436 F. Supp. 3d at 729; *United States v. Ulbricht*, 2014 WL 5090039, at \*13-15 (S.D.N.Y. Oct. 10, 2014), *aff'd* 858 F.3d 71 (2d Cir. 2017); *United States v. Blakstad*, 2020 WL 5992347, at \*7-8 (S.D.N.Y. Oct. 9, 2020). In so ruling, the courts have relied upon the well-reasoned opinion in *In re A Warrant for All Content & Other Info. Associated with the Email Account xxxxxxxx@Gmail.com Maintained at Premises Controlled by Google, Inc.*, 33 F. Supp. 3d at 388 (S.D.N.Y. 2014). In that case, the court upheld a warrant for all emails from a service provider. The court started from the well-established propositions that (1) “[there is a long-recognized] practical need for law enforcement to exercise dominion over documents not within the scope of the warrant in order to determine whether they fall within the warrant,” *id.* at 392, and (2) that “[i]n the case of electronic evidence, which typically consists of enormous amounts of undifferentiated information and documents, . . . a search for documents or files responsive to a warrant cannot possibly be accomplished during an on-site search,” *id.* at 393. It reasoned that there is no “constitutionally significant difference between the searches of hard drives [which of necessity must be conducted offsite] . . . and searches of email accounts” and thus that “the case

law . . . concerning searches of hard drives and other storage media [and permitting them to be seized for later review offsite] supports the Government’s ability to access an entire email account in order to conduct a search for emails within the limited categories contained in the warrant.” *Id.* at 394. The court specifically addressed and rejected the proposition that law enforcement would be required to have the email host conduct the search of emails: in the absence of “a limitation in the scope of the items to be seized [that] would allow the email host to produce responsive material in a manner devoid of the exercise of skill or discretion, for example, under a warrant requiring disclosure of all emails from a particular time period, . . . it is unrealistic to believe that Google or any other email host could be expected to produce the materials responsive to categories listed in a search warrant.” *Id.* at 394. “First, the burden on Google would be enormous because duplicating the Government’s efforts might require it to examine every email.” *Id.* “Second, Google employees would not be able to interpret the significance of particular emails without having been trained in the substance of the investigation.” *Id.* at 395.

Both the Email and the iCloud Search Warrant track and are modelled on the warrants routinely approved in this Circuit. They identify the time period for which the service provider is required to produce information and limit law enforcement to searching that information for emails or messages that are evidence of the identified Subject Offenses. They also are supported by affidavits that link the time period and the evidence to be seized to evidence of the Subject Offenses. If they are not more limited, that is because the evidence as set forth in the affidavits cannot reasonably be set forth in any other manner that would permit the service provider to produce the information suspected to provide evidence of the Subject Offenses in a manner that would be “devoid of the exercise of skill or discretion.” *Id.* at 394.

The Court recognizes that in *Blake*, the Eleventh Circuit held that a similar warrant for information possessed by Facebook was overly broad because it sought all information from the accounts without any limiting search terms, time periods, or categories of information. 868 F.3d at 966-967. The court concluded that the warrants should have permitted law enforcement to obtain data only from the time period that defendants took part in the prostitution conspiracy at issue in the case and only with respect to persons who had been identified as being involved in the criminal activity. *Id.* at 973-974. The court stated that “[d]isclosures consistent with those limitations might then have provided probable cause for a broader, although still targeted, search of [the defendant’s] Facebook account.” *Id.* at 974. It concluded such procedure was necessary to “undermin[e] any claim that the Facebook warrants were the internet-era version of a ‘general warrant.’” *Id.*

The Court respectfully declines to follow *Blake* to the extent that it would require the service provider to limit the messages subjected to the warrant to those between persons whom law enforcement already identified as being involved in the Subject Offenses. That holding would be inconsistent with the law of this Circuit. *Blake* is based on the implicit premise that law enforcement can and should articulate relevant search terms or criteria—such as messages to and from a specific person—in advance and that it must limit itself to obtaining from the service provider only those messages that fall within the parameters it can identify in advance. It thus envisions a process whereby the Government would start with a narrow search, only to continuously return back to the magistrate judge with an ever-expanding list of search terms as each narrow search slowly yielded additional persons and communications specifically identified as being relevant to the subject offenses. So understood, the Fourth Amendment would require a different standard for searching messages within an email or social media account than, for

example, for searching documents and records within a physical premises—such as a home or an office. In a home or an office, as Judge Gorenstein and others have pointed out, the Fourth Amendment “sanctions some perusal, generally fairly brief, of . . . documents (seized during an otherwise valid search) . . . in order for the police to perceive the relevance of the documents to crime.” *In re A Warrant for All Content & Other Info. Associated with the Email Account xxxxxxxx@Gmail.com Maintained at Premises Controlled by Google, Inc.*, 33 F. Supp. 3d at 388 (quoting *United States v. Mannino*, 635 F.2d 110, 115 (2d Cir. 1980)); *see also Ulbricht*, 2014 WL 5090039, at \*14 (“It has long been perfectly appropriate to search the entirety of a premises or object as to which a warrant has issued based on probable cause, for specific evidence as enumerated in the warrant, which is then to be seized.”) Defendant’s argument here, however, would allow law enforcement the right to peruse only those emails or instant messages whose specific relevance had already been determined in advance. For the reasons outlined by Judge Gorenstein, the Court believes that such limitation is not required by the Fourth Amendment.

Ray also argues that the foregoing decisions supporting the right of law enforcement to seek and obtain a warrant for an entire email or social media account for a particular period predate, and are no longer good law under, the Supreme Court’s decisions in *Riley v. California*, 573 U.S. 373 (2014) and *Carpenter v. United States*, 138 S. Ct. 2206 (2018). Dkt. No. 137 at 1. Ray asserts that these Supreme Court cases, and others, “represent a shift in the law,” adapting the Fourth Amendment to technological innovations. *Id.* But—leaving aside that many of the decisions relied upon by the Government here postdate *Riley* and *Carpenter*—*Riley* and *Carpenter* involve only the questions of whether probable cause is required to conduct a search of cellphone data and the identity of the person who can claim a legitimate expectation of privacy in such information. They do not involve the question whether—as here—after law

enforcement has made a showing that there is probable cause that a federal crime has been committed and has established probable cause that the email accounts and social media accounts will contain evidence of the identified offenses, an issuing magistrate is still required to limit the communications that law enforcement can seize to those that law enforcement has already identified and cannot give law enforcement authority to seize the communications of which it is not yet aware but nonetheless constitute evidence of the crime. Magistrate judges have long been permitted to give the executing officer that power in the case of physical documents and a long line of cases in this Circuit address that question in the case of electronic documents in a way that is favorable to the Government here and not to Ray.

Finally, for the reasons largely discussed above in connection with the seizure of electronic devices from the 40 Holly Lane Premises, the searches conducted of the email and iCloud accounts also fall within the “good faith” exception to the exclusionary rule. Law enforcement presented detailed evidence supporting probable cause to a neutral magistrate who was exercising a judicial role and obtained a warrant limited in time that permitted law enforcement to seize only limited and prescribed messages and emails. That warrant was consistent with other warrants that had been approved in this Circuit. What the court said in *Blake* in rejecting suppression as a remedy even after holding that the warrants failed the particularity requirement, also necessarily applies here: “[P]robable cause supported issuance of the warrants” and whether the warrants violated the particularity requirement “is not an open and shut matter.” 868 F.3d at 975. “[I]t is a close enough question that the warrants were not ‘so

facially deficient’ that the FBI agents who executed them could not have reasonably believed them to be valid.” *Id.*<sup>2</sup>

**F. Ray’s Challenge to the Nexus between the asserted probable cause for the Premises Search Warrant and the Premises**

Ray argues that the affidavit in support of the Premises Search Warrant did not demonstrate probable cause that he lived at 40 Holly Lane at the time of the warrant’s issuance or that there was probable cause to believe that evidence of a crime could be located at that location. Taking each piece of evidence piecemeal, Ray argues that the information in the warrant did not demonstrate probable cause that he was residing at the premises because “the recent information relating to the location was too vague, while the more specific information relating to the location was too stale.” Dkt. No. 137 at 24. He argues that the affidavit did not reference any database, driver’s license record, utility bill, lease agreement, or other official record showing that Ray lived at 40 Holly Lane and that there was no recent history of Ray using the address for shipping or billing. Dkt. No. 110 at 56. In the alternative, Ray asks for a hearing under *Franks v. Delaware*, 438 U.S. 154 (1978), to assess the legality of the warrants.

Ray’s argument rests on an implicit misstatement of the approach that the issuing magistrate must take in determining whether probable cause exists and the approach this Court must follow in determining whether there was a “substantial basis” for the magistrate judge’s

---

<sup>2</sup> The Court also rejects Ray’s argument that having properly seized the email and iCloud accounts for review at law enforcement premises, law enforcement was required to apply only search terms pre-approved by an issuing judge. *See Nejad*, 436 F. Supp. 3d at 728 (the rationale that permits law enforcement to review hard drives offsite “applies with equal force to email accounts such that courts in this district have ‘upheld the Government’s ability to obtain the entire contents of [an] email account to [later] determine which particular emails come within the search warrant.’” ) (quoting *In re A Warrant for All Content & Other Info. Associated with the Email Account xxxxxx@Gmail.com Maintained at Premises Controlled by Google, Inc.*, 33 F. Supp. 3d at 394).



determination. The probable cause analysis does not require the issuing magistrate to take each piece of evidence one by one and blind herself to it if each piece of evidence does not establish probable cause when taken in isolation or is too dated or ambiguous. The officer examines all of the evidence together and determines based on the “totality of the circumstances” whether probable cause exists. *Gates*, 462 U.S. at 230-31. Law enforcement also is not required to produce formal documentation or copies of a criminal’s correspondence with retail outfits to establish the “practical, common-sense” determination that “there is a fair probability that contraband or evidence of a crime will be found in a particular place.” *Id.* at 238. Those engaged in criminal activity do not ordinarily advertise their address to outsiders. Law enforcement can rely on observations, reports, and inferences.

The evidence set forth in the affidavit was sufficient to establish probable cause that evidence of crime would be located at 40 Holly Lane and to show Ray lived at that location. As of the date of the warrant, his presence at that location was not transient or momentary or “a one-time occurrence.” *Wagner*, 989 F.2d at 75. Ray was present at the 40 Holly Lane address on numerous occasions from at least October 2018 (if not earlier)<sup>3</sup> to February 7, 2020, the date of the Premises Search Warrant Affidavit.

Ray argues that the fact he “was near 40 Holly Lane the day before the search does not establish probable cause that he lived at that address when the warrant was issued.” Dkt. No. 137 at 26. He also argues that the report from the PPD indicates he was present at 40 Holly Lane in May 2019 but not that he was a “resident” there in May 2019. *Id.* at 27. But the police

---

<sup>3</sup> The Premises Search Warrant Affidavit recites evidence from Uber Technologies, Inc. that FV-2 requested rides as early as September 2016 to and from addresses neighboring 40 Holly Lane; that beginning in May 2016, Associate-1 requested rides to and from addresses neighboring 40 Holly Lane; and that starting in May 2017, FV-2 and Associate-1 requested rides to and from 40 Holly Lane.

received information from a victim that in late 2018 Ray was residing in Piscataway, and in October 2018, Ray himself represented he was living there. Just months before the search at issue in this case his relative's car was in the driveway of the residence. In light of the evidence that Ray was engaged in "continuing criminal activity," *Wagner*, 989 F.2d at 75, as well as the statements from the warrant that evidence of Ray's past criminal activity was of the type that would be maintained for months if not years, there was probable cause to search the 40 Holly Lane Premises. *See Scott v. United States*, 2019 WL 6034973, at \*5 (S.D.N.Y. Nov. 14, 2019) (finding that there was probable cause for June 2012 search of residence where the search warrant affidavit "described numerous instances in August 2011 when [defendant] emerged from the Residence to sell crack-cocaine to a confidential informant").

Even if the warrant were not supported by probable cause, the agent relied in good faith on the warrant in conducting the search of the Subject Premises. *Clark*, 638 F.3d at 100. Ray does not argue that the issuing judge abandoned his judicial role in authorizing the warrant. *Id.* (identifying the standards necessary to demonstrate the "wholesale abandonment of the judicial role discussed in *Leon*"). The warrant also was not so facially deficient that the executing officers could not reasonably presume it to be valid. *Id.* at 101 ("a warrant is facially defective when it omits or misstates information specifically required to be contained therein"). It specifically identified the place to be searched and specifically identified the items that could be seized. *Id.* Nor was the warrant affidavit so lacking in indicia of probable cause "as to preclude reasonable reliance." *Id.* It contained "detailed factual allegations in support of probable cause." *Id.* at 103. Even assuming a "thoughtful[] and competent[] judge[]" might disagree as to whether the facts alleged established probable cause," that would not be enough to invalidate the officers' reliance on the warrant. *Id.* at 104 (quoting *Leon*, 468 U.S. at 926).

Nor is Ray entitled to a *Franks* hearing. Ray has not made the required “substantial preliminary showing that a deliberate falsehood or a statement made with reckless disregard for the truth was included in the warrant affidavit and the statement was necessary to the judge’s finding of probable cause.” *United States v. Falso*, 544 F.3d 110, 125 (2d Cir. 2008). Ray argues that, in the Premises Search Warrant Affidavit, the agent falsely swore that she had “reviewed records from the Piscataway Police Department (the ‘PPD’), reflecting that law enforcement officers from the PPD conducted a welfare check at the subject premises in May 2019, and learned that Ray resides at the subject premises.” Dkt. No. 137 at 27 (quoting Dkt. No. 110-1 at 263).

The police records do not state that Ray lived at the 40 Holly Lane Premises. The contemporaneous incident report states: “3 females and 1 male inside house // parents state that isabella has hist of suicide attempts // isabella pollak 27 yof (hist of suicide) / lauren ray / lawrence ray / felicia rozario.” Dkt. No. 137, Ex. A. at 2. Thus, though the incident report indicates that Ray was inside the 40 Holly Lane Premises at the time of the wellness check, it does not report that he resided there. A record of an interview with Rosario and Pollak two days later stated that relatives of Rosario and Pollak has come to the house and “knocked on their door looking for ‘Larry.’” *Id.* These are the only references to Ray in the PPD police reports.

Although the statement that the police records reflected that Ray resided at the 40 Holly Lane Premises was inaccurate, the defense has not met its burden of showing that the agent’s statement was a deliberate falsehood or was made with reckless disregard for the truth. The thrust of the police records is substantially similar to the truth; the records reported that Ray was inside the house at the time of the wellness check and that when Pollak and Rosario spoke with police on May 3, they indicated that their relatives had come to the house looking for “Larry.”

Though the records do not state that Ray “resided” there as the agent reported on the Premises Search Warrant Affidavit, the mistake is not a large one and is not particularly important to the determination of probable cause. If the agent had correctly reported what was in the records, there still would have been probable cause to search the 40 Holly Lane Premises.

**G. Ray’s Argument that there was insufficient probable cause to search the Storage Unit for electronics.**

Ray also challenges the probable cause to search the Storage Unit for electronics. He does not dispute that there was probable cause for the agents to search the Storage Unit itself. The affidavit supporting the Storage Unit Warrant plainly established probable cause to believe that evidence of the Subject Offenses would be located in the Storage Unit. It included the statements of one of the alleged victims that she “kept journals in which [she and others] wrote about their alleged wrongdoing to Ray and his family members and associates,” and that “Ray moved the journal and many other items, including items of sentimental value, to storage bins” in the Storage Unit after he moved to the Subject Premises. Dkt. No. 110-1 at 320. The information was corroborated by the agent’s observation of “many locked and closed containers” inside the Storage Unit. *Id.* at 321. That was sufficient to establish probable cause. Moreover, even if the Storage Unit Warrant Affidavit did not establish probable cause, Ray does not dispute that the agents relied in good faith on the warrant signed by the issuing judge in entering the Storage Unit.

Ray argues that the agent’s observation that “Ray [wa]s likely to store computers, cellphones and electronic devices” in the Storage Unit was insufficient to permit the issuing judge to authorize the officers to seize electronic devices because it was based solely on the assertion that the agent saw an “early model Apple laptop” in the Storage Unit. Dkt. No. 112 at 31. He

contends that since all that the agent swore was that she saw an “early model Apple laptop” in the Storage Unit and since Apple started making laptops in 1991, “potentially decades older than any of the alleged criminal conduct,” the statement was insufficient to support probable cause to permit the search and seizure of electronic devices at the storage area. *Id.* at 51. No allegation is made about the age of the electronic devices that were seized at the Storage Unit.

Ray’s argument fails for three independent reasons. First, the agents did not need to establish probable cause that there would be electronic devices in the Storage Unit for the warrant to authorize them to seize electronic devices if they were found there. To pass constitutional muster, a search warrant affidavit must establish probable cause to believe that a crime was committed and that the premises to be searched contain the evidence, fruits, or instrumentalities of criminal activity and the warrant itself must contain a “description of the objects to be seized” that is no “broader than can be justified by the probable cause upon which the warrant is based.” *Galpin*, 720 F.3d at 446 (quoting 2 W. LaFare, *Search and Seizure* § 4.6(a) (5th ed. 2012)). The affidavit need not establish that there is probable cause that each item identified to be evidence of the crime is at a particular location. The magistrate judge can authorize law enforcement to seize an item of evidence that there is probable cause to believe would be at one of a number of different locations without establishing the existence of probable cause that it currently is present at any one of the locations. *See, e.g., United States v. Souza*, 2008 WL 753736, at \*18 (E.D.N.Y. Mar. 19, 2008) (holding that probable cause may extend to multiple locations based upon the same evidence).

Ray relies upon *Zurcher v. Stanford Daily*, 436 U.S. 547 (1978) for the proposition that, in order to execute a lawful search of the electronic devices in the storage area, the warrant must have included probable cause to believe that there would be electronic devices in the storage area

that would have evidence of the subject offenses. *See id.* at 556 (“The critical element in a reasonable search is not that the owner of the property is suspected of crime but that there is reasonable cause to believe that the specific ‘things’ to be searched for and seized are located on the property to which entry is sought.”). This language is divorced from its context. In *Zurcher*, the issue was the validity of a warrant to search the offices of a newspaper that was believed to have photographic evidence of demonstrators assaulting police officers; thus, the language from *Zurcher* which Ray quotes merely illustrates that a warrant can lawfully issue to search the property of individuals who are not suspected of any crime, if there is probable cause to believe that such individuals possess evidence of a crime. *See id.* at 558 (“[V]alid warrants to search property may be issued when it is satisfactorily demonstrated to the magistrate that fruits, instrumentalities, or evidence of crime is located on the premises.”). It has nothing to do with the specificity required in a warrant. *See id.* at 565 (“Properly administered, the preconditions for a warrant—probable cause, specificity with respect to the place to be searched and the things to be seized, and overall reasonableness—should afford sufficient protection against the harms that are assertedly threatened. . . .”).

Furthermore, it stands to reason that *Zurcher* cannot stand for what Ray argues it does. The intrusion into privacy that is effected by a search is justified by the notion that, when the police enter space as authorized by a warrant, they will find evidence of a crime there. Of course, the warrant must contain a sufficient degree of specificity to ensure that the warrant is not a general one. But as long as there is a connection between what the police are searching for and the criminal activity they are investigating, there need not be a likelihood that the materials they are searching for are in any particular place.

The search of the Storage Unit satisfied the standards of the Fourth Amendment. The Storage Unit Search Warrant Affidavit established probable cause to believe that Ray had committed the Subject Offenses (he was indicted for them). It also established probable cause to believe that the Storage Unit contained the evidence, fruits and instrumentalities of the Subject Offenses. Finally, it established probable cause to believe that electronic devices—to the extent they were found in the Storage Unit—would both be themselves evidence and an instrumentality of the Subject Offenses and also would be likely to contain further evidence, fruits and instrumentalities of the Subject Offenses. The agent swore that based on her training and experience “individuals who engage in the Subject Offenses commonly use electronic devices to communicate with co-conspirators,” identified evidence that Ray himself used electronic devices in the commission of the Subject Offenses, and further swore based on training and experience that “evidence of the criminal activity can often be found months or even years after it occurred.” Dkt. No. 110-1 at 327-28. It was required to do no more.

Second, once the agents were in the Storage Unit lawfully pursuant to the search warrant, they had the authority to seize the electronic devices that were in plain view. *See Horton v. California*, 496 U.S. 128, 134-35 (1990) (holding that the police “may seize evidence in plain view . . . [where] the police have a warrant to search a given area for specified objects, and in the course of the search come across some other article of incriminating character.”).

Finally, regardless whether probable cause was in fact needed to believe that electronic devices were contained in the Storage Unit, the agents relied in good faith on the warrant and thus suppression would not be the appropriate remedy even if there were a constitutional violation. *Leon*, 468 U.S. at 905.


In response to the Government's contention that the search of the Storage Unit was "independently justified by consent" because FV-2 gave permission for the officers to search it, Dkt. No. 118 at 13-14, Ray argues that the Government has failed to show that FV-2 ever gave such consent. Dkt. No. 137 at 29. Ray argues that the Government has failed to show that FV-2 consented, because, although the Storage Unit Search Warrant Affidavit stated that FV-2 gave her permission, the FBI 302 report of her statements does not say that she consented. But the fact that the statement was not reported in the 302 report does not mean that the claim in Storage Unit Search Warrant Affidavit is false. The 302 report says nowhere that she did not consent; it is silent with respect to the issue. Accordingly, the 302 report has nothing to do with probable cause for the Storage Unit Search Warrant. More importantly, Ray has put forth no evidence that there was any falsity in the Storage Unit Search Warrant Affidavit's claim that FV-2 consented. The fact that FV-2's consent was not recorded in the 302 report does not provide evidence of such falsity on its own.

### **CONCLUSION**

For the reasons stated, the Court DENIES the motions to suppress. The Clerk of Court is respectfully directed to close the motion at Dkt. No. 109.

SO ORDERED.

Dated: May 26, 2021  
New York, New York

---

LEWIS J. LIMAN  
United States District Judge